Traitement Quantique de l'Information

Draft version hiver 2013 - 2014

Nicolas Macris

Contents

Introduction

Le traitement de l'information et le calcul sont de façon ultime un processus physique. En effet l'information est stockée et traitée dans des systèmes biologiques (systèmes vivants), mécaniques (machine de Babbage), électroniques (ordinateurs modernes), optiques etc.

Néanmoins en théorie de l'information et du calcul classique on peut dans une large mesure s'affranchir des lois de la physique des systèmes sous-jacents. Ainsi, il suffit généralement de retenir uniquement l'aspect mathématique du concept "d'information". C'est ce qui rend cette théorie universelle et dans une large mesure indépendante de la technologie utilisée. Seules quelques hypothèses physiques de bases sont retenues. Par exemple, la notion de bit classique est basée sur la stabilité et la reproductibilté de signaux de bases ainsi que sur la possibilité d'effectuer des mesures sans perturber l'état du système. Une tension électrique ou bien un domaine magnétique sont assez stables pour pouvoir être modélisés par un signal digital bien défini $x \in \{0, 1\}$. De plus il est en principe possible de mesurer et d'observer l'état $x \in \{0, 1\}$ sans occasionner de perturbation significative.

Néanmoins, les composants des systèmes électroniques et optiques de traitement de l'information s'approchent des tailles nanométriques et les limites de validité de la physique classique sont atteintes. Le traitement de l'information stockée aux échelles de distances et de temps atomiques ou moléculaires doit tenir compte des lois de la physique quantique valable à ces échelles. En effet le caractère universel et purement mathématique de la théorie de l'information classique n'est plus valable à ces échelles et doit être repensé pour tenir compte des lois naturelles quantiques. En fait des changements conceptuels radicaux par rapport aux concepts classiques sont nécessaires. La notion de bit classique, $x \in \{0, 1\}$, qui est l'unité de base de l'information classique, doit être complètement révisée. Nous introduirons la notion de "bit quantique" - le qubit - qui possède un caractère "à la fois discret et continu". Très curieusement, nous verrons qu'un bit quantique est un vecteur à deux composantes complexes continues, mais qui répond de facon discrète quand il s'agit d'en extraire de l'information! Le qubit est l'unité de base de l'information quantique. Les notions d'observation, de mesure et de stabilité d'un état du qubit doivent également être révisées en profondeur.

La nouvelle discipline qui décrit valablement le traitement de l'information

et son implémentation aux échelles atomiques ou moléculaires porte le nom *Information et Calcul Quantique*. Les technologies associées au développement de cette discipline sont encore naissantes et le plus souvent limitées à des expériences de laboratoires. Mais les concepts et les idées de base de l'information et du calcul quantique sont apparues dans les travaux pionniers de Landauer, Bennioff, Feynman, Bennett, Wiesner, Deutsch et d'autres il y a maintenant, déjà presque quarante ans (circa 1980). Ces travaux n'étaient pas forcément motivés par des développements technologiques mais plutôt par des réflexions scientifiques profondes sur la nature physique de l'information et du calcul, et notamment les limites de principe imposées par les lois de la physique (notamment les lois de la thermodynamique et de la physique quantique). Dans les vingts dernières années le sujet a connu un essor fulgurant suite aux progrès expérimentaux dans la réalisation de certains protocoles de transmission d'information quantique, et aussi suite au développement théorique de l'algorithme (de P. Shor) quantique de factorisation en temps polynomial. Ces aspects fondamentaux formeront quelques uns des chapitres principaux du cours.

La partie I est une introduction élémentaire à la physique quantique. Aucun prérequis n'est nécessaire, mis à part quelques notions de base d'algèbre linéaire. La physique quantique est née des découvertes expérimentales qui révolutionnèrent la physique au tournant du 19ème au 20ème siècle. Le développement de la théorie quantique est le fruit d'un long processus initié entre autres dans les travaux de M. Planck, A. Einstein, N. Bohr, L. de Broglie, E. Schroedinger, M. Born, E. Heisenberg, P. Dirac entre 1900 et 1930. La formulation moderne de la théorie exposée au chapitre 4 fut développée par P. Dirac et J. von Neumman à la fin de cette époque, et est essentiellement inchangée encore aujourd'hui.

Le chapitre 1 est une description semi-historique des expériences de base (les expériences d'interférences et l'effet photoélectrique) mettant en évidence la dualité onde-particule. Cette nature duale de la matière est à la base de la notion d'état quantique et forme aussi la base de la notion de bit quantique - le qubit - lequel possède une nature duale continue/discrète. Le qubit généralise la notion de bit classique et forme l'unité de base de la théorie de l'information et du calcul quantique.

La nature abonde de degrés de liberté qui sont exactement ou approximativement représentés par des qubits. Ainsi les qubits sont une ressource naturelle! Deux exemples fondamentaux de qubits exacts sont introduits dans le chapitre 2: la polarisation des photons et le spin 1/2 des électrons. Certains des principes de la physique quantique sont illustrés sur ces exemples.

Le chapitre 3 introduit de façon plus formelle les lois quantiques et les éléments du formalisme mathématique que nous utiliserons. En théorie de l'information et calcul quantique nous avons principalement besoin du formalisme quantique pour des degrés de liberté discrets et nous nous limitons donc à ce cadre, ce qui est en fait une grande simplification. La mécanique quantique des degrés de liberté continus ne sera pas abordée dans ce cours, bien que le sujet soit bien sûr très important. La situation est analogue au cas classique où le traitement

digital de l'information ne requiert pas ou très peu de la théorie du traitement des signaux continus.

La partie II constitue une introduction aux aspects fondamentaux de l'information et du calcul quantique.

Les chapitres 4 et 5 introduisent les protocoles à la base de la théorie des communications quantiques. Tout d'abord nous exposons au chapitre 4 le célèbre protocole de Bennett et Brassard (1984) qui permet la distribution d'une clé secrète entre deux acteurs distants Alice et Bob. L'étude de ce protocole est une bonne illustration du "postulat de la mesure" (introduit aux chapitres 2 et 3) de la physique quantique.

Le chapitre 5 aborde les protocoles de "codage superdense" et de "téléportation". Ces protocoles très importants mettent en évidence une ressource nouvelle présente en information quantique et qui n'a pas de contrepartie classique. Cette ressource provient de la possibilité "d'intriquer" deux systèmes (les qubits d'Alice et Bob par exemple). Comme nous le verrons l'intrication est une forme de corrélation qui n'a pas d'analogue classique: en particulier ce type de corrélation quantique - appelée intrication - ne peut pas être décrit par des variables aléatoires classiques. Nous verrons comment cela suit des inégalités de J. Bell (1964) et des expériences d'Aspect-Grangier-Roger (1981).

Le calcul et les algorithmes quantiques sont introduits aux chapitres 6 et 7. Dans le chapitre 6 nous introduisons un modèle de calcul populaire dû à D. Deutsch (1985) - le modèle des circuits quantiques - qui est en fait une généralisation du modèle classique des circuits. Les circuits quantiques sont constitués de "portes logiques quantiques" universelles généralisant les portes classiques AND, OR, XOR, TOFFOLI et permettant de simuler une large classe de "calculs". Dans cette optique un algorithme quantique est un circuit initialisé dans un état approprié de plusieurs qubits et produisant un état de sortie. Le processus de mesure (d'observation) sur l'état sortant des qubits produit le résultat du calcul. Comme nous le verrons ce processus de mesure donne un résultat aléatoire, et de ce point de vue les algorithmes quantiques sont des algorithmes aléatoires. Néanmoins le circuit quantique lui-même est déterministe.

L'agorithme le plus spectaculaire est probablement l'algorithme de Shor (1994) permettant de factoriser des entiers en temps polynomial dans le nombre de bits (ou décimales) de l'entier. Cet algorithme est étudié en détail dans le chapitre 8. Les meilleurs algorithmes classiques connus à ce jour nécessitent un temps quasi-exponentiel. Par rapport à ces algorithmes classiques l'algorithme de Shor offre une accélération quasi-exponentielle du temps de calcul. Cela suit de la possibilité de traiter des qubits intriqués en parallèle grâce aux circuits quantiques. La complexité du problème de la factorisation est à la base des systèmes de cryptographie à clé publique et l'apparition d'un ordinateur quantique capable d'implémenter l'algorithme de Shor serait révolutionnaire.

La partie III aborde la question de l'implémentation réelle de systèmes d'information quantique. Concernant les protocoles de communication tels que la distribution de clé, le codage superdense ou la téléportation il existe déja une technologie

naissante basée sur la production, la manipulation et la transmission d'états quantiques des photons. Par exemple, la faisabilité de protocoles de distribution de clé secrète (similaires au protocole de Bennett et Brassard) a été démontrée sur des distances d'une centaine de kilomètres. L'étude de ces expériences nécessiteraient d'aborder l'optique quantique qui est bien au delà du cadre de ce cours. Nous nous concentrons ici sur la réalisation des portes logiques et des circuits quantiques par résonnance magnétique nucléaire (RMN). Dans ces réalisations expérimentales les qubits sont des moments magnétiques nucléaires, et ceux-ci sont manipulés grâce à des impulsions électromagnétiques. Le cadre de la RMN permet d'aborder quelques réalisations expérimentales existantes et notamment l'implémentation de l'algorithme de Shor pour un petit nombre de qubits (de l'ordre de la dizaine). Le défi majeur est aujoud'hui de travailler avec un grand nombre de qubits (de l'ordre de $10^4 - 10^7$). Pour cela des technologies plus appropriées que la RMN sont explorées dans les laboratoires, mais leur discussion dépasse largement le cadre de ce cours. Néanmoins les principes de la manipulation de qubits sont similaires à ceux que nous allons étudier dans le cadre de la RMN.

Le chapitre 8 aborde la dynamique du spin 1/2 dans des champs magnétiques. Cela nous permettra de décrire l'implémentation des portes logiques à un qubit telles que NOT et Hadamard (cette dernière n'a pas d'analogue dans les circuits classiques).

Le chapitre 9 aborde la question des portes à deux qubits telles que XOR ou Control-NOT. Cette implémentation est beaucoup moins facile dans la mesure où il faut controller l'interaction entre deux qubits. Heureusement, comme nous le verrons, la nature nous offre des interactions appropriées entre moments magnétiques (interactions de Heisenberg).

Le chapitre 10 conclu le cours par un survol de la réalisation de circuits et d'algorithmes quantiques. Nous discutons brièvement des expériences implémentant avec succès l'algorithme de Shor pour une dizaine de qubits ($\sim$ 2000).

Comme expliqué plus haut réaliser un ordinateur quantique pouvant traiter de l'ordre de $10^4 - 10^7$ qubits est aujourd'hui un défi majeur. La raison tient au fait que plus le nombre de degrés de libertés du système augmente plus la "cohérence" de l'état quantique est perdue à cause des interactions du système avec son environnement, et le système se comporte alors de plus en plus comme un système obéissant aux lois de la physique classique. C'est le problème de la décohérence déja discutée par Schroedinger en 1935 sous la forme d'un paradoxe, celui du "chat de Schroedinger". La décohérence sera discutée brièvement à la fin du cours. En deux mots, la question est de savoir si un système macroscopique - un chat ou un ordinateur quantique - peut être maintenu ou non assez longtemps (ou plus précisément pendant combien de temps) dans un état quantique cohérent? Bien que la réponse ne soit pas entièrement claire la plupart des physiciens s'accordent aujourd'hui pour affirmer qu'il n'y a en principe pas d'obstacles de principe pour maintenir la cohérence quantique d'un système si ses degrés de liberté sont suffisamment bien isolés de leur environnement. Les seuls obstacles

à la réalisation d'un ordinateur quantique manipulant un nombre appréciable de qubits seraient donc d'ordre purement technologique.

Je tiens à remercier David Blanchet et Thomas Rubelli qui ont contribué á la préparation de ces notes ainsi que de nombreux étudiants pour leurs questions, remarques et commentaires.

Part I

I. Introduction à la Théorie Quantique

1 La Dualité Onde-Particule

1.1 Introduction

La mécanique quantique fut établie à travers un long processus expérimental et conceptuel au début du 20ème siècle ($\sim$ 1900-1930). En 1900, l'édifice de la physique classique semblait complet avec d'une part les lois de la mécanique Newtonienne décrivant le mouvement des particules matérielles, et d'autres part la théorie de Maxwell décrivant tous les phénomènes électromagnétiques. La distinction entre particule et onde était nette. Par exemple on considérait que l'électron est une particule possédant une position $\vec{x} = (x, y, z) \in \mathbb{R}^3$ bien définie, une vitesse et quantité de mouvement (ou impulsion) bien définie $\vec{p} = m\vec{v}$ ($\vec{v} = \frac{\mathrm{d}\vec{x}}{\mathrm{d}t}$). Etant donné des conditions initiales $\vec{x}(0)$ et $\vec{v}(0)$ on peut décrire grâce à l'équation différentielle de Newton la trajectoire $\vec{x}(t)$ (et aussi $\vec{v}(t)$). La précision attribuée à cette description n'est qu'une "affaire de technologie" et on peut espérer repousser toute incertitude grâce à des instruments de plus en plus précis. D'autre part, suite aux travaux de Maxwell et aux expériences de Hertz il était établi que la lumière visible est une onde électromagnétique, de même nature que les ondes radio; la seule différence étant l'ordre de grandeur de la longueur d'onde et la fréquence. Les ondes électromagnétiques sont des vibrations ondulatoires des champs électriques et magnétiques décrites par les équations (aux dérivées partielles) de Maxwell. Celles-ci sont parfaitement déterministes, et l'évolution du champ électromagnétique est connu en tout temps, si on sait fixer les conditions initiales.

Les expériences qui furent à l'origine d'une véritable révolution conceptuelle, et menèrent à un changement complet de paradigme, concernent l'interaction de la matière et du rayonnement.

Tout d'abord en 1900 la distribution spectrale des fréquences dans un "corps noir" mena Planck à considérer que la lumière est absorbée et émise par les parois matérielles en quantités discrètes. La théorie électromagnétique des ondes prédisait un échange continu d'énergie et était incapable de reproduire le bon spectre de fréquence du corps noir[1].

Ensuite "l'effet photoélectrique" fut clairement mis en évidence par Lénard en 1902 (suite aux travaux antérieurs de Hertz $\approx$ 1885) et conduisit Einstein à

[1] Un “corps noir” est une cavité matérielle (comme un four) dont les parois sont en équilibre thermique avec la radiation. Nous n'en dirons pas plus dans ce cours

postuler que la lumière est en fait constituée de corpuscules, aujourd'hui appelés "photons". Nous reviendrons sur l'effet photoélectrique.

L'observation de raies spectrales (d'émission ou d'absorption) discrètes pour divers éléments chimiques indiquait aussi que l'échange d'énergie entre atomes et radiation est de nature discrète. Bohr (1910) repris la nouvelle idée de photon et proposa le "modèle de Bohr de l'atome". Sa théorie permettait d'expliquer les raies spectrales connues et même d'en prédire de nouvelles qui furent observées beaucoup plus tard. Nous reviendrons sur ces questions.

Etant donné que la lumière semblait avoir une nature à la fois corpusculaire et ondulatoire, De Broglie postula que cela pourrait être le cas pour les électrons aussi; et en fait pour toute forme de matière. En 1924 il proposa une formule associant une longueur d'onde (appelée aujourd'hui longueur d'onde de De Broglie) aux électrons. Grâce à cette formule, les résultats de Bohr à propos des raies spectrales (de l'Hydrogène) pouvaient être reproduit. Les idées de De Broglie furent confirmées expérimentalement par Davisson et Germer par des expériences de diffraction d'électrons sur des cristaux. Ces expériences (1927) confirmèrent de façon éclatante et surprenante que les électrons peuvent parfois se comporter comme des ondes.

Entre 1925-1930 la théorie quantique moderne, encore universellement utilisée aujourd'hui, fut développée par Schroedinger, Heisenberg, Born, Jordan, Dirac (et d'autres...). Schroedinger (1926) élabora (à partir des idées de De Broglie) l'équation régissant l'évolution temporelle de "l'onde de De Broglie" associée aux particules. Cela lui permit de calculer de façon fondamentale le spectre de l'atome d'hydrogène. Aujourd'hui on sait que l'équation d'onde de Schrodinger est à la base de la chimie. Heisenberg (1925-26) développa une approche différente, plus directement basée sur les propriétés connues à l'époque de l'interaction entre atomes et rayonnement (par exemple les raies spectrales, etc.). Son approche était abstraite et conduisait à décrire la position et l'impulsion des électrons orbitant autour du noyau par des matrices. Sa mécanique était appelée "mécanique des matrices". Born, Jordan et Dirac montrèrent très rapidement que les approches de Schroedinger et Heisenberg étaient en fait des formalismes mathématiquement équivalents.

Aujourd'hui les physiciens font à peine la distinction entre les deux approches, ondulatoire et algébrique. En fait elles furent largement unifiées dans les travaux de Dirac et von Neuman ($\sim$ 1930-1932) qui présentèrent une formalisation et un cadre mathématiquement précis des lois de la mécanique quantique. Cette formalisation sera présentée dans le chapitre 3. Elle reste à ce jour essentiellement inchangée et donne un cadre mathématique clair pour la description des phénomènes. Ce chapitre 1 ainsi que le chapitre 2 donnent une première introduction à quelques concepts à partir de la phénoménologie expérimentale. Ainsi, la formalisation mathématique de la théorie quantique (chap 3) paraîtra moins arbitraire.

Le cheminement historique brièvement décrit ci-dessus est à la fois trop long et compliqué pour être décrit en détail ici. Nous allons donc introduire deux aspects

essentiels de la phénoménologie quantique en sélectionnant deux expériences clés. Celles-ci sont : l'expérience des fentes de Young et l'effet photoélectrique.

1.2 Les expériences de doubles fentes

L'expérience de Young - 1803

La nature ondulatoire de la lumière fut d'abord mise en avant par Hooke, Huygens et Euler. Néanmoins Newton pensait que celle-ci était constituée de corpuscules et c'est cette conception qui domina jusqu'au 19ème siècle. Ce débat fut (provisoirement!) clos par Young en 1803 qui établit de manière expérimentale que la lumière est une onde et fut notamment capable de déterminer la longueur d'onde de la lumière visible (rouge, vert, bleu, etc...).

Le schéma de l'expérience est esquissé sur la figure 1.1.

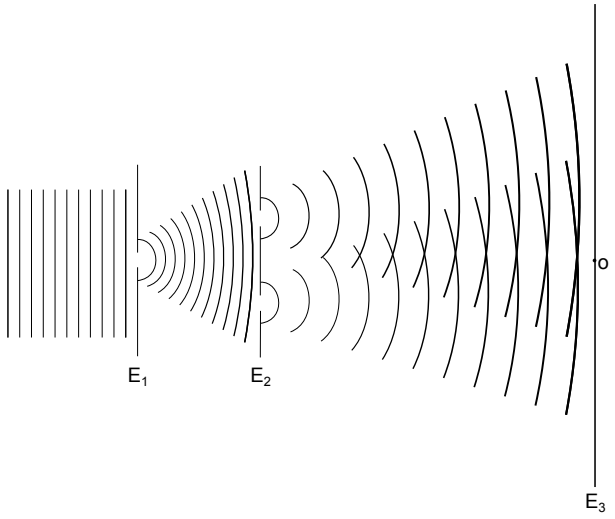


Figure 1.1 Expérience de doubles fentes

Un faisceau monochromatique est envoyé sur un écran E_1 percé par une fente. Le faisceau est diffracté et arrive en E_2. Cette étape sert simplement à travailler avec une source cohérente ponctuelle constituée par la fente de E_1 . La lumière est ensuite diffractée par les deux fentes de E_2 qui se comportent comme deux sources ponctuelles. Si $\vec{r}_1$ et $\vec{r}_2$ sont les positions des deux fentes, les deux ondes sphériques sortantes des fentes ont la forme

$$\psi_1(\vec{r}) = A\frac{e^{i(k|\vec{r}-\vec{r}_1|-\omega t)}}{|r-\vec{r}_1|} \tag{1.1}$$

et

$$\psi_2(\vec{r}) = A\frac{e^{i(k|\vec{r}-\vec{r}_2|-\omega t)}}{|r-\vec{r}_2|}. \tag{1.2}$$

Ici $\psi_1(\vec{r})$ et $\psi_2(\vec{r})$ sont les amplitudes des deux ondes au point $\vec{r}$ de l'espace. Le nombre d'onde k est relié à la longueur d'onde par $k = \frac{2\pi}{\lambda}$ et ω est relié à la fréquence de l'onde $\omega = 2\pi\nu$. Pour la lumière on a $\lambda\nu = \frac{\omega}{k} = c$ où $c \approx 2.997 \times 10^8$ m/s est la vitesse de la lumière (dans le vide). La figure montre des cercles qui représentent les maximas des deux amplitudes (l'espace entre les cercles correspond aux minimas). Ces deux ondes "se superposent". Le principe de superposition de la théorie des ondes stipule que l'amplitude totale au point $\vec{r}$ est donnée par

$$\psi(\vec{r}) = \psi_1(\vec{r}) + \psi_2(\vec{r}). \tag{1.3}$$

En d'autres termes les maximas se renforcent quand les cercles s'intensifient. Cela produit les "figures d'interférence" avec lesquelles nous sommes tous familiers à condition d'être un peu observateur. En effet des figures d'interférence peuvent être observées en jetant deux cailloux sur la surface d'un lac plat! Toujours est-il qu'une observation plus précise est obtenue, comme le fit Young, en récoltant l'intensité lumineuse sur l'écran E_3. L'intensité récoltée est donnée par $|\psi(\vec{r})|^2$ où $\vec{r} \in E_3$. Il sera montré aux exercices que

$$|\psi(\vec{r})|^2 \simeq \frac{4A^2}{D^2}\cos^2(\frac{\pi d}{\lambda}\frac{\rho}{D}), \qquad D >> d, \tag{1.4}$$

où D est la distance entre E_2 et E_3, d la distance entre les deux fentes ($d = |\vec{r_1} - \vec{r_2}|$) et ρ la variable radiale mesurée à partir du centre de l'écran (point O). Les franges d'interférence sont circulaires. La figure 1.2 représente une coupe radiale de l'intensité en fonction de ρ.

Les maximas de l'intensité se trouvent sur les cercles concentriques de rayons $\rho_n = n\lambda\frac{D}{d}$. La distance entre deux maximas est $\rho_{n+1} - \rho_n = \lambda\frac{D}{d}$. En mesurant cette distance, Young était capable de déterminer λ. Pour la lumière visible λ est de l'ordre de 600 à 400 nm (1 nm = 10^-9 m).

Que se passerait-il si le faisceau lumineux était constitué d'un ensemble de projectiles ("des grains de lumière") ou de corpuscules? La prédiction “naïve classique” donnerait un élargissement du faisceau au passage des fentes à cause des collisions avec le bord des fentes. On s'attendrait à trouver plus de particules au centre de chaque faisceau diffracté et moins au bord (voir figure). L'intensité récoltée en E_3 ne présenterait pas de franges d'interférences. Vous pouvez essayer de faire l'expérience avec des balles de tennis ou de ping-pong. Vous pouvez lancer ces balles une par une, ou toutes ensemble à travers les fentes; cela ne change pas grand chose aux résultats de la figure 1.3. L'intensité récoltée sur E_3 (nombre de balles en fonction de la position) à la forme $N_1(\vec{r}) + N_2(\vec{r})$ (figure 1.4). Mais la

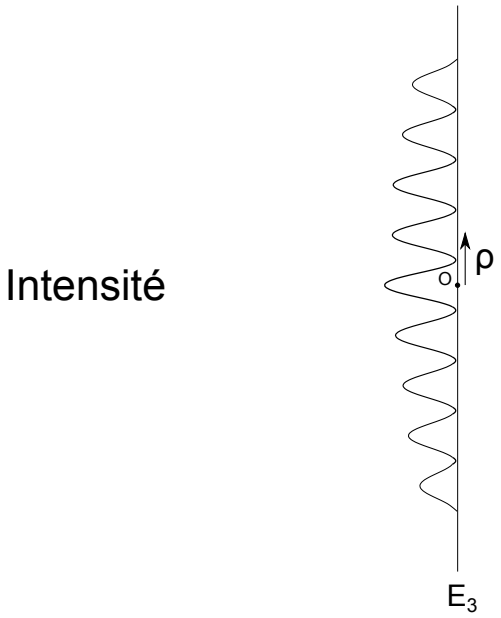


Figure 1.2 Intensité

nature est très surprenante en fait! Dans le paragraphe suivant nous discutons des expériences modernes de Young faites avec des électrons et même des molécules.

Expériences modernes de doubles fentes - post 1960

En 1909 G. Taylor répéta l'expérience de Young avec une source de lumière très faible, correspondant à la lumière d'une bougie placée à environ 1 km de l'écran! La figure d'interférence est toujours observée. À l'époque, on ne pouvait pas conclure grand chose de cette expérience, mis à part le fait que la nature ondulatoire de la lumière est valable même pour des intensités très très faibles. Nous allons voir qu'en fait l'expérience de Taylor préfigure des expériences modernes absolument remarquables faites avec des particules. En effet comme nous le verrons dans le paragraphe sur l'effet photoélectrique, on sait aujourd'hui que les sources d'intensité très faibles sont des sources de photons (corpuscules de lumière).

En 1961, C. Jönsson parvint à réaliser l'expérience des doubles fentes avec des électrons. Les franges d'interférence sont observées et cela suggère que les électrons se comportent comme une onde. En fait une chose très surprenante est aussi observée : si nous envoyons les électrons un par un à travers les fentes on observe des points d'absorption aléatoires sur l'écran E_3. En attendant un certain temps on observe que l'ensemble de ces points forme une figure d'interférence.

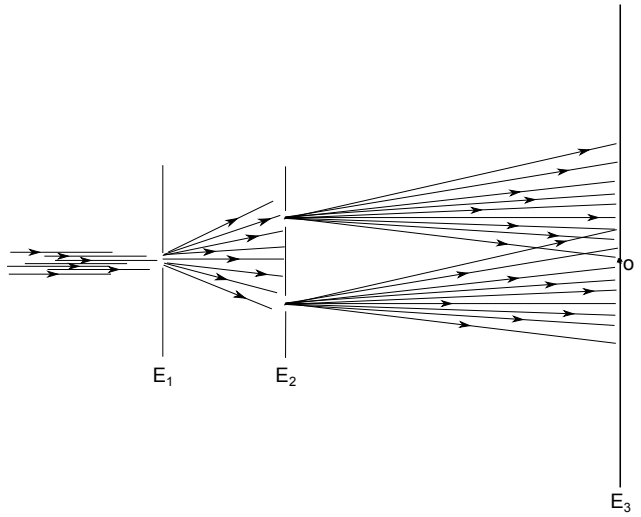


Figure 1.3 Résultat de l'expérience

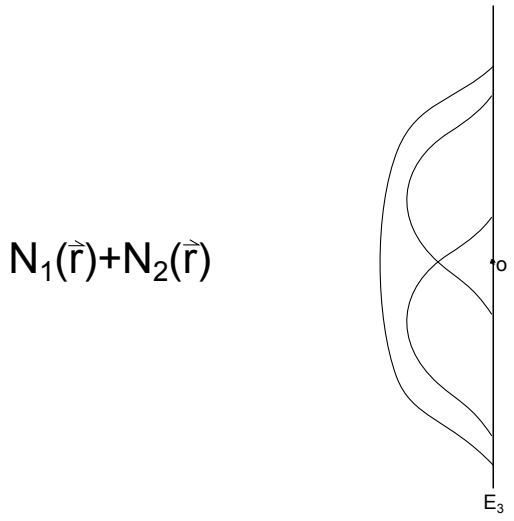


Figure 1.4 Intensité en $E3$

Ainsi il semble que l'électron est ponctuel au moment où son absorption est observée sur l'écran. Mais la distribution statistique des points d'absorptions satisfait à la figure d'interférence! Les électrons se comportent donc aussi comme des ondes.

Cette expérience a été réalisée aussi avec des neutrons et en 1999 avec des molécules de Carbone 60. Ces molécules sont "grosses", elles contiennent 60 atomes de carbone arrangés de manière sphérique sur les sommets de 12 pentagones et 20 hexagones (elles sont donc des mini-ballons de foot). Le diamètre d'une telle molécule est d'environ 0.7 nm (alors que l'on ne sait pas associer une dimension à l'électron; on dit qu'il est "ponctuel"). Encore plus récemment, il y a deux ans, des expériences ont été réalisées avec d'autres types de molécules artificielles contenant entre 400 et 1000 atomes. À chaque fois, sous certaines conditions expérimentales, les franges d'interférence sont observées! Ces grosses molécules se comportent donc comme des ondes. La distance entre les maximas des franges d'interférence permet d'associer une longueur d'onde λ à ces molécules (en acceptant la formule $\rho_{n+1} - \rho_n = \lambda \frac{D}{d}$ dérivée précédemment). Etonnamment on trouve une longueur d'onde beaucoup plus petite (quelques centaines de fois plus petite) que la taille des molécules elles-mêmes. La description ondulatoire du passage des molécules à travers ces fentes a-t-elle encore un sens? La physique quantique moderne stipule que oui! (Il est permis d'être sceptique; mais en même temps il faut savoir que la physique quantique passe tous les tests expérimentaux par ailleurs).

Ces expériences confirment de façon éclatante que les particules matérielles possèdent sous certaines conditions un comportement ondulatoire. Mais pourquoi est-ce que cela n'est pas le cas avec une balle de tennis ou de ping-pong ou un ballon de foot; pourquoi n'observe-t-on pas de franges d'interférence? Où se situe la limite entre l'électron, le C60, les molécules à 400-1000 atomes et les ballons de foot ou les corps macroscopiques? Cette question est profonde et mal comprise. On ne sait pas très bien répondre à la question de savoir où se situe la limite entre comportement quantique dual "ondulatoire-corpusculaire" et le comportement classique non-dual (ondulatoire ou corpusculaire). Les expériences modernes des doubles fentes avec les grosses molécules permettent d'étudier cette question, et c'est là que réside tout l'intérêt de ces expériences.

Il a été mis en évidence que lorsque les molécules de C60 interagissent trop fortement avec leur environnement (par exemple en échangeant de la radiation avec leur environnement) les franges d'interférence disparaissent. En d'autres termes la caractéristique ondulatoire est préservée à condition que les molécules de C60 soient suffisamment bien isolées de leur environnement. Lorsque ceci n'est pas le cas les physiciens parlent de "décohérence". La décohérence est le processus de perte de cohérence des ondes quantiques à travers l'interaction d'un système avec son environnement. Une très grosse molécule, ou un ballon de football est constamment en interaction avec l'environnement et possède donc un comportement classique.

Comme nous le verrons à la fin de ce cours, construire un ordinateur quantique serait un peu comme réaliser une expérience de Young avec des ballons de football tellement bien isolés de leur environnement que des franges d'interférence seraient observées! En effet, la plupart des physiciens pensent que les comportements

quantiques s'appliquent à toute forme de matière, à toute échelle, tant que le système est suffisamment bien isolé pour que la décohérence n'opère pas.

1.3 L'effet photoélectrique

L'effet photoélectrique concerne l'interaction de la lumière avec la matière. Quand la fréquence de la radiation devient assez grande (typiquement à partir des ultraviolets mais aussi dans le visible et dans les infrarouges) on observe que cette interaction est de nature discrète. Il existe plusieurs effets qui mettent cela en évidence (L'effet Compton, la création de paires, etc...), mais historiquement l'effet photoélectrique fut le premier à être découvert.

En 1885 Hertz étudie l'éclair produit par des ondes radio sur une bobine. Il observe que curieusement la longueur de l'éclair est plus courte quand l'installation est placée dans une chambre noire ; et plus longue quand l'expérience est réalisée à la lumière du jour. A l'époque ces résultats étaient peu clair et Hertz abandonna cette expérience. On sait aujourd'hui que les rayons ultraviolets contenus dans la lumière du jour contribuaient à intensifier l'éclair en arrachant des électrons aux atomes environnants. Ce n'est qu'en 1902 que cet effet fut observé clairement par Lénard qui illuminait des gaz avec de la lumière ultraviolette. Au dessus d'une fréquence critique (dans l'ultraviolet) des électrons sont arrachés aux atomes de gaz, un courant est observé dans un circuit couplé au système. De plus Lénard parvint à montrer que l'énergie cinétique des électrons arrachés augmentait avec la fréquence de la radiation. Cette énergie cinétique semblait indépendante de l'intensité de la radiation (le courant électrique, ou en d'autres termes le nombre d'électrons arrachés par unité de seconde, est lui proportionnel à l'intensité de la radiation).

Ces résultats furent interprétés par Einstein dans un de ses fameux articles en 1905. Celui-ci postula que la radiation est constituée de corpuscules - aujourd'hui appelés photons. Il associa à ces photons une énergie et une quantité de mouvement

$$E = h\nu \qquad \text{et} \qquad p = \frac{h}{\lambda}, \tag{1.5}$$

où λ et ν sont la longueur d'onde et la fréquence de radiation. Ici $h \simeq 6.63 \times 10^{-24}$ J·s est la constante de Planck. En fait, Planck avait déjà introduit une idée connexe, ainsi que la constante h, dans son étude du corps noir. Celui-ci supposait que les échanges d'énergie entre la matière et la radiation électromagnétique sont discrets et multiples de $h\nu$. Néanmoins Planck ne concevait pas que la radiation électromagnétique puisse être constituée de particules; les photons. Ainsi, c'est Einstein qui a introduit le premier la dualité onde-corpuscule pour la radiation électromagnétique.

Selon Einstein l'énergie cinétique des électrons arrachés au métal vaut (voir figure 1.5)

$$\frac{1}{2}mv^2 = \begin{cases} h\nu - W_0 & h\nu > W_0, \\ 0 & h\nu < W_0. \end{cases} \tag{1.6}$$

W_0 est l'énergie minimale qu'il faut pour arracher un électron au gaz. Si on pose $h\nu = W_0$ on trouve la fréquence critique $\nu_0 = \frac{W_0}{h}$ en-deça de laquelle il n'y a pas d'effet photoélectrique. L'expression ci-dessus repose sur 3 hypothèses; (i) la conservation de l'énergie; (ii) le fait que l'énergie d'un photon vaut $h\nu$ et (iii) W_0 est indépendant de la fréquence et de l'intensité de la radiation. La conservation de l'énergie est une loi universellement valable en physique et n'a jamais été remise en question jusqu'ici. En revanche (ii) et (iii) ne sont pas évidents a priori. L'hypothèse (iii) est valable dans un régime approprié et n'a pas le statut de loi fondamentale. D'ailleurs il serait assez difficile de déterminer W_0 par un calcul fondamental. Quand à (ii), Energie du photon = $h\nu$ est une loi fondamentale de la physique.

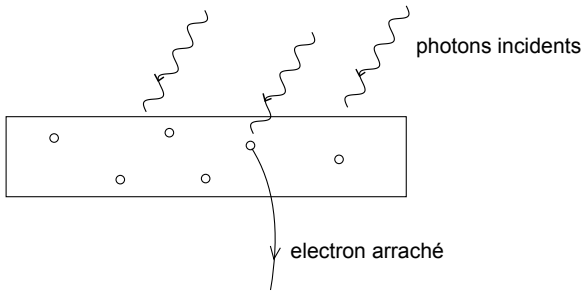


Figure 1.5 Electron arraché avec des photons

Bien que simple, en 1905 cette formule était révolutionnaire. En effet elle stipule que la radiation est constituée de quantas élémentaires (les photons) et que leur énergie dépend (linéairement) de la fréquence uniquement; et non pas de l'intensité lumineuse. La théorie de Maxwell quand à elle, prédit que l'énergie est proportionelle à l'intensité. Il est possible de réconcilier ces théories en réalisant qu'une onde électromagnétique classique doit être associée à plusieurs photons dont l'énergie est $Nh\nu$. On montre alors que le nombre de photons N est relié à l'intensité de l'onde.

La relation linéaire en fréquence qu'Einstein (suite au travaux de Planck)

postula n'était pas évidente à partir des résultats expérimentaux de Lénard. Ce n'est qu'en 1934 que R.A. Millikan réussit à faire des expériences bien controllées qui vérifièrent cette relation linéaire.

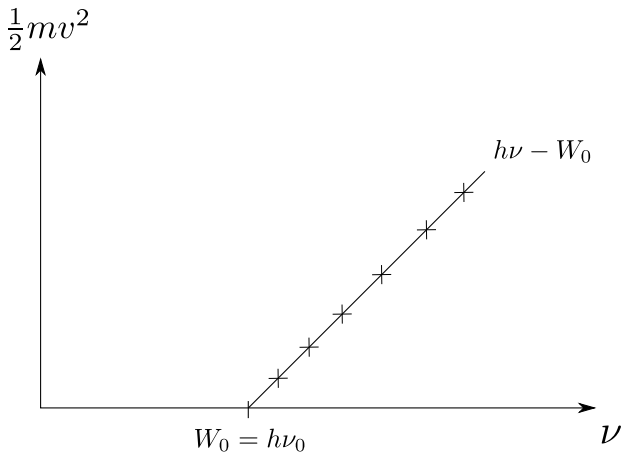


Figure 1.6 Relation linéaire de l'expérience de Millikan

Millikan réussit aussi à déterminer la constante de Planck expérimentalement à partir de la pente de la courbe (une droite). (La valeur numérique de $h = 6.63 \times 10^{-24}$ J $\cdot$ s. Notons 1 J $= 6.2 \times 10^{18}$ eV, et $13,6$ eV est l'énergie necessaire pour arracher un électron à l'atome d'hydrogène.

L'expérience de Young et l'effet photoélectrique mettent en évidence des aspects complémentaires du comportement de la lumière. Ensemble, ils établissent que la lumière possède un comportement dual. Au début du 20ème siècle ceci était tellement révolutionnaire que la théorie d'Einstein mis du temps à être acceptée, même après les expériences de Millikan.

Revenons un instant à l'expérience de Taylor de 1909. Celui-ci observait une figure d'interférence pour une lumière d'intensité si faible qu'il devait attendre environ six mois avant de voir les franges d'interférence se constituer. La raison est que les photons arrivent par petits nombres sur les deux fentes puis l'écran. De nos jours il est possible de contrôler assez précisément des sources de photons essentiellement uniques.

1.4 La "fonction d'onde": une révolution conceptuelle

L'effet photoélectrique et l'expérience de Young montrent que la lumière (le champ électromagnétique) possède un comportement dual. En 1924 De Broglie

conjectura que ceci pouvait aussi être le cas pour des électrons et en fait pour toute matière. Les expériences d’interférence modernes (de double fente) montrent de façon spectaculaire que cela est bien le cas.

De Broglie associa à la particule une longueur d’onde λ et une fréquence ν données par la relation

$$\lambda = \frac{h}{p}, \qquad \text{et} \qquad \nu = \frac{E}{h}. \tag{1.7}$$

Ce sont essentiellement les mêmes relations que pour un photon. Mais ici, pour une particule non relativiste de masse m on a $p = mv$ et $E = \frac{1}{2}mv^2 = \frac{p^2}{2m}$ (où v est la vitesse de la particule).

Plus généralement: *on peut associer à la particule une onde d’amplitude* $\psi(\vec{r}, t)$. Nous discutons d’abord deux exemples simples, puis l’interprétation de cette “fonction d’onde”.

Si la particule n’est soumise à aucune force et que son mouvement est dans la direction z, il est naturel de lui associer l’onde plane (par analogie aux ondes électromagnétiques)

$$\psi(\vec{r}, t) = Ae^{2\pi i(\frac{z}{\lambda} - \nu t)} = Ae^{\frac{i}{\hbar}(pz - Et)} \tag{1.8}$$

où $\hbar = \dfrac{h}{2\pi}$.

Pour une particule dans l’expérience des doubles fentes l’onde sera sphérique:

$$\psi_{1,2}(\vec{r}, t) = A\frac{e^{\frac{i}{\hbar}(p|\vec{r} - \vec{r}_{1,2}| - Et)}}{|\vec{r} - \vec{r}_{1,2}|} \tag{1.9}$$

La "fonction d’onde" ou "amplitude" totale est donnée par le principe de superposition

$$\psi(\vec{r}, t) = \psi_1(\vec{r}, t) + \psi_2(\vec{r}, t) \tag{1.10}$$

La différence cruciale avec la théorie classique des ondes est qu’ici la "fonction d’onde" décrit une seule particule unique.

Quelle est l’interpétation de $\psi(\vec{r}, t)$? Max Born suggéra peu après l’introduction de la fonction d’onde (la fonction d’onde prend des valeurs complexes et ci-dessous on prend le module au carré du nombre complexe)

$$|\psi(\vec{r}, t)|^2 \tag{1.11}$$

représente *la densité de probabilité* de trouver la particule en $\vec{r}$ au temps t. En d’autres termes la quantité

$$\int_V \mathrm{d}^3\vec{r} \quad |\psi(\vec{r},t)|^2 \tag{1.12}$$

est la probabilité de trouver la particule dans une région $V \subset \mathbb{R}^3$. Pour que cette interprétation soit consistante il faut bien sûr imposer la condition de normalisation

$$\int \mathrm{d}^3\vec{r} \quad |\psi(\vec{r},t)|^2 = 1 \tag{1.13}$$

En général cette condition peut toujours être satisfaite en ajustant la constante de normalisation A.

Cette interprétation est parfaitement consistante avec les expériences de doubles fentes. Lorsque les particules sont envoyées une par une à travers les fentes on observe des points d'absorption bien localisés sur l'écran. Ces points sont aléatoires. Quelle est leur distribution statistique? L'ensemble des points d'absorption forme des franges d'interférence d'intensité proportionnelle à $|\psi(\vec{r},t)|^2$. On en déduit que la distribution de probabilité des points d'absorption est donnée par la règle de Born $|\psi(\vec{r},t)|^2$.

1.5 Première notion "d'état quantique"

En un mot l'"état quantique" est une abstraction ou bien une généralisation de la notion de "fonction d'onde". Nous discutons cette généralisation dans ce paragraphe. La fonction d'onde est un état associé aux degrés de liberté continus (telle que la position). Au chapitre 2 nous allons introduire des états quantiques associés à des degrés de liberté discrets. Ce sont en fait ces degrés de liberté discrets qui nous intéressent vraiement en information quantique. Nous verrons aussi que les états associés aux degres de liberté sont les "quantum bits".

Le concept de fonction d'onde et la règle de Born étaient vraiment révolutionnaires. On abandonne la notion de trajectoire pour les particules. Les concepts de position ou de vitesse bien déterminés font encore sens uniquement si on ne les mesure pas simultanément. Par exemple lorsque l'on observe le point d'absorption sur l'écran celui-ci est aléatoire : la position est observée, mais la direction de propagation au moment de l'absorption a perdu son sens.

En mécanique quantique l'état de la particule est décrit par une fonction d'onde. On peut penser à cette fonction de façon plus abstraite comme à un vecteur de l'espace des fonctions. Ce vecteur ou état est noté

$$|\psi\rangle \quad \longleftrightarrow \quad \psi(\vec{r}). \tag{1.14}$$

Cette notation est la notation traditionnelle de la MQ introduite par Dirac; on pourrait aussi noter $\vec{\psi}$, mais $|\psi\rangle$ est conventionel. Le mérite de cette notation est peut être de nous rappeler que les vecteurs d'états ne vivent pas dans l'espace

physique familier à trois dimensions. Le symbole $|\psi\rangle$ s'appelle aussi un "ket". Le vecteur transposé et complexe conjugué $\vec{\psi}^{T,*}$ s'appelle un "bra" et est noté

$$\langle\psi| \quad \longleftrightarrow \quad \psi^*(\vec{r}). \tag{1.15}$$

Le produit scalaire entre un vecteur et son propre transposé est la norme au carré de ce vecteur. Ici on a

$$\langle\psi|\psi\rangle = \int \mathrm{d}^3\psi^*(\vec{r})\psi(\vec{r}) = \int \mathrm{d}^3\vec{r} \quad |\psi(\vec{r})|^2. \tag{1.16}$$

L'interprétation de Born impose $\int \mathrm{d}^3\vec{r} \quad |\psi(\vec{r})|^2 = 1$ (probabilité totale égale à un). Ainsi un vecteur d'état doit satisfaire à la condition, dite de normalisation

$$\langle\psi|\psi\rangle = 1.$$

Ces considérations suggèrent que plus généralement le produit scalaire entre deux vecteurs $|\psi\rangle$ et $|\phi\rangle$ jouera un role important en MQ. Pour des vecteurs d'états correspondants à des fonctions d'onde le produit scalaire naturel (naturel à cause de la règle de Born! en effet du point de vue purement mathématique on aurait pu définir d'autres produits scalaires!) est

$$\langle\phi|\psi\rangle = \int \mathrm{d}^3\vec{r} \quad \phi^*(\vec{r})\psi(\vec{r}). \tag{1.17}$$

Ce produit scalaire satisfait aux règles usuelles de linéarité, symmétrie et positivité.

Lorsqu'une particule est observée localisée en $\vec{r_1}$ son vecteur d'état est noté $|\vec{r_1}\rangle$. On peut de facon un peu cavalière, penser à ce vecteur d'état comme étant celui qui correspond à la "fonction de Dirac" (ou distribution)

$$|\vec{r_1}\rangle \quad \longleftrightarrow \quad \delta(\vec{r} - \vec{r_1}) \tag{1.18}$$

Notons maintenant qu'en vertu du produit scalaire introduit ci-dessus

$$\langle\vec{r}|\psi\rangle = \int \mathrm{d}^3\vec{r} \quad \delta(\vec{r} - \vec{r_1})\psi(\vec{r}) \qquad\qquad = \psi(\vec{r}). \tag{1.19}$$

Ainsi nous avons la connection suivante entre la notation des "bras" et "kets" et celle de la fonction d'onde

$$\langle\vec{r}|\psi\rangle = \psi(\vec{r}). \tag{1.20}$$

En fait la d'érivation ci-dessus est un peu cavalière (essayez de dire pourquoi) et il faut prendre cette dernière relation comme la définition du bra $|\vec{r}\rangle$. De même on définit le ket $|\vec{r}\rangle$ via

$$\langle\psi|\vec{r}\rangle = \psi^*(\vec{r}). \tag{1.21}$$

Nous allons maintenant donner une formulation un peu plus générale de la règle de Born. Rappelons-nous que la densité de probabilité d'observer la particule en $\vec{r}$ quand son état est $|\psi\rangle$ est donnée par

$$|\psi(\vec{r})|^2 = |\langle\vec{r}|\psi\rangle|^2 \tag{1.22}$$

En mécanique quantique le "postulat de la mesure" généralise cette règle. Nous donnerons au chapitre 3 une formulation complètement précise de ce postulat. Pour le moment (chap 1 et 2) nous allons nous contenter de la formulation suivante:

"La probabilité d'observer l'état final $|\phi\rangle$ juste aprés une mesure, lorsque l'état initial du système est $|\psi\rangle$ juste avant la mesure, est donnée par $|\langle\phi|\psi\rangle|^2$."

Lorsque nous étudierons la formalisation de la mécanique quantique nous verrons que le bon cadre formel est celui des espaces de Hilbert. Nous verrons entre autres que:

(i) Les états quantiques sont des vecteurs. Il est possible d'additionner deux vecteurs, ce qui correspond à la superposition de deux fonctions d'onde.
(ii) Les produits scalaires donnent les probabilités observées lors des mesures.

Ces règles seront précisées au chapitre 3.

1.6 Principe d'incertitude de Heisenberg

Une caractéristique fondamentale de la mécanique quantique est l'impossibilité de déterminer avec une précision infinie la position et l'impulsion d'une particule. Une expression mathématique de ce fait est donnée par le principe d'incertitude que nous discutons ici.

Nous avons vu que pour une particule dans l'état $|\psi\rangle$, la probabilité de trouver la particule en x est $|\psi(x)|^2$ (On considère le cas à une dimension spatiale $x \in \mathbb{R}$). L'incertitude ou l'écart type obtenu lors de mesures répétées est alors

$$\sigma_x = \left\{ \int \mathrm{d}x \;\; x^2 |\psi(x)|^2 - \left(\int \mathrm{d}x \;\; x|\psi(x)|^2 \right)^2 \right\}^{\frac{1}{2}} \tag{1.23}$$

Les physiciens écrivent plutôt δx au lieu de σ_x.

Supposons maintenant que l'on mesure l'impulsion p de la particule. Quel est le ket $|p\rangle$ correspondant à une particule d'impulsion p ? En fait la fonction d'onde associée à ce ket $|p\rangle$ est l'onde plane $e^{\frac{i}{\hbar}px}$. Notez que la densité de probabilité associée est $|e^{\frac{i}{\hbar}px}|^2 = 1$, donc cette fonction d'onde est complètement délocalisée dans l'espace. Aussi, puisque par définition $\langle\vec{r}|\psi\rangle = \psi(\vec{r})$ nous avons

$$\langle x|p\rangle = e^{\frac{i}{\hbar}px}. \tag{1.24}$$

Si l'état observé est $|\psi\rangle$ la probabilité de trouver une impulsion mesurée p est (règle de Born généralisée)

$$|\langle p|\psi\rangle|^2 = \int \mathrm{d}x \;\; e^{-\frac{i}{\hbar}px}\psi(x) = |\hat{\psi}(p)|^2 \tag{1.25}$$

où $\hat{\psi}$ est essentiellement la transformée de Fourier de ψ. Ainsi $|\hat{\psi}(p)|^2$ est une densité de probabilité pour l'impulsion de la particule. L'incertitude peut être définie comme

$$\sigma_p = \left\{ \int \mathrm{d}p \;\; p^2 |\hat{\psi}(p)|^2 - \left(\int \mathrm{d}p \;\; p|\hat{\psi}(p)|^2 \right)^2 \right\}^{\frac{1}{2}} \tag{1.26}$$

A nouveau les physiciens notent δp au lieu de σ_p.

Etant donné une fonction de carré sommable, c.a.d $\int \mathrm{d}x \;\; |\psi(x)|^2$ fini[2] un théorème de mathématique affirme que

$$\sigma_x \, \sigma_p \geq \frac{\hbar}{2}. \tag{1.27}$$

Cette inégalité souvent écrite $\delta x \, \delta p \geqslant \frac{\hbar}{2}$ est le principe d'incertitude d'Heisenberg. L'interprétation physique est qu'il est impossible de mesurer avec précision infinie x et p en même temps avec un même appareil de mesure (par exemple un "microscope"). Si on gagne en précision pour x on perd en précision pour p et vice-versa. Ce n'est pas un problème de limitation dû à l'instrument de mesure, mais une limitation intrinsèque imposée par les lois quantiques.

1.7 Le problème des raies spectrales

Lorsque la lumière visible passe à travers un prisme on observe un spectre continu de couleurs. Plus généralement le spectre des ondes électromagnétiques est continu.

En 1885 Balmer mis en évidence que l'hydrogène et les atomes en général, possèdent un spectre d'émission discret. Pour l'hydrogène Balmer détectait 4 raies dans les longueurs d'onde de la lumière visible $\lambda = 656.3$ nm; 481.1 nm; 434.1 nm et 410 nm. Elles satisfont à la formule empirique

$$\frac{1}{\lambda} = R_H \, (\frac{1}{4} - \frac{1}{m^2}), \qquad m = 3, 4, 5, 6 \tag{1.28}$$

avec $R_h = 10973731,57 \text{ m}^{-1}$.

Le problème qui se posait était d'expliquer cette formule donnant des longueurs d'onde discrètes décrites par le nombre entier m. Nous allons voir qu'en fait cette formule est un cas particuler d'une formule générale proposée par Bohr.

[2] Notez que le théorème de Parseval affirme $\int \mathrm{d}x \;\; |\psi(x)|^2 = \int \mathrm{d}p \;\; |\hat{\psi}(p)|^2$

La formule de Bohr prédisait toute une série d'autres raies spectrales qui furent observées pour certaines d'entre elles bien plus tard.

Les expériences célèbres de Rutherford (diffusion de particules α sur des feuilles d'or) avaient démontré en 1903 que les atomes sont constitués d'un noyau chargé positivement (charge Ze) et de Z électrons (charge e) "orbitant" autour du noyau. Néanmoins la stabilité de ce "système planétaire" ne pouvait pas être expliqué par les lois de la physique classique. En effet une charge orbitant autour d'un centre doit rayonner et perdre de l'énergie si bien qu'au bout d'un temps (très long) elle tombe sur le noyau.

Les idées quantiques naissantes permirent, sinon d'expliquer la stabilité des atomes, de justifier la formule de Balmer et de la généraliser. Cela fut d'abord établi par Bohr. Celui-ci postula que (i) l'électron peut orbiter autour de certaines "trajectoires permises" et (ii) les lois de la mécanique classique s'appliquent à ces trajectoires permises. Ensuite il donna une "règle de quantification" pour toutes ces "trajectoires permises". Cette règle sera discutée aux exercices; ici nous suivons une approche due à De Broglie basée sur le concept de fonction d'onde.

Sur une trajectoire permise supposée circulaire on a :

$$m\,\frac{v^2}{R} = k\,\frac{Ze^2}{R^2} \tag{1.29}$$

et

$$E = \frac{1}{2}mv^2 - k\,\frac{Ze^2}{R} \tag{1.30}$$

où v est la vitesse, m la masse, k la constante de Coulomb, E l'énergie mécanique et R le rayon de la trajectoire. A partir de ces formules il est facile de montrer que l'énergie associée à la trajectoire de rayon R est :

$$E = -\frac{k}{2}\frac{Ze^2}{R}. \tag{1.31}$$

Maintenant il s'agit de trouver les rayons des trajectoires permises. Selon De Broglie l'onde associée à l'électron le long de sa trajectoire doit être stationnaire (c'est-à-dire que les noeuds doivent être immobiles). Pour une trajectoire circulaire la condition de stationnarité est :

$$n\lambda = 2\pi R, \qquad n \geq 1 \tag{1.32}$$

où λ est la longueur d'onde et n un entier[3]. Pour λ on pose suivant De Broglie:

[3] Comme pour une corde de violon de longueur $2\pi R$: $n = 1$ donne la note fondamentale et $n = 2, 3, 4, ...$ donnent les harmoniques

$$\lambda = \frac{h}{p} = \frac{h}{mv} \tag{1.33}$$

Puisque $v = \left(\frac{k}{m}\frac{Ze^2}{R}\right)^2$ on obtient $\lambda = \frac{hR^{\frac{1}{2}}}{(kmZe^2)^{\frac{1}{2}}}$ et donc

$$R = \frac{\hbar^2}{kmZe^2}\, n^2, \qquad n \geq 1 \tag{1.34}$$

Pour les rayons permis. Cela donne

$$E_n = -\frac{k^2 Z^2 e^4 m}{2\hbar^2}\frac{1}{n^2} = -\mathrm{Ry}\,\frac{Z^2}{n^2}; \qquad n \geq 1. \tag{1.35}$$

Ici $\mathrm{Ry} = \dfrac{k^2 e^4 m}{2\hbar^2} \simeq 13.6$ eV est la constante de Rydberg. Pour l'Hydrogène on a en particulier $Z = 1$.

Les énergies E_n des trajectoires permises s'appellent les "niveaux d'énergies" et forment le "spectre" de l'atome d'Hydrogène (Pour $Z = 1$). Comme nous l'avons dit la notion de trajectoire n'a pas vraiment de sens. Mais remarquablement cette formule est exacte pour l'hydrogène. Ceci fut établi par Schrödinger et est discuté brièvement dans le prochain paragraphe.

Revenons aux raies spectrales. Toujours selon Bohr, un électron peut transiter d'une orbite "numéro m" à une orbite "numéro n" en émettant un photon d'énergie $E_m - E_n$. La fréquence du photon sera donnée par la relation d'Einstein

$$h\nu_{m\to n} = E_m - E_n \tag{1.36}$$

Puisque $E_n = -\frac{\mathrm{Ry}}{n^2}$ (on prend $Z = 1$ pour l'Hydrogène) on trouve

$$h\nu_{m\to n} = -\left(\frac{\mathrm{Ry}}{m^2} - \frac{\mathrm{Ry}}{n^2}\right) \tag{1.37}$$

avec $\lambda\nu = c$ pour le photon on trouve

$$\frac{1}{\lambda_{m\to n}} = \frac{\mathrm{Ry}}{hc}\left(\frac{1}{n^2} - \frac{1}{m^2}\right) \tag{1.38}$$

la constante $\dfrac{\mathrm{Ry}}{hc} = R_H$ (la constante de Balmer). Les raies de Balmer correspondent à la série des transitions $m \to 2$ ($n = 2$). La série $m \to 1$ s'appelle série de Lyman (et fut observée aussi tard qu'en 1914; ultraviolets). La série $m \to 3$ est la série de Paschen et correspond à l'infrarouge. Le nombre de ces raies spectrales est infini, et le point important est qu'elles sont discrètes.

1.8 L'équation de Schroedinger- complément facultatif

Comme nous l'avons vu l'approche dite "semi-classique" utilisée au paragraphe 1.7 n'est pas très satisfaisante conceptuellement car elle fait encore appel à la notion classique de trajectoire.

Schrödinger dériva en 1926 sa fameuse équation qui décrit la dynamique de la fonction d'onde $\psi(\vec{r},t)$. En résolvant son équation il était capable de trouver la condition de stationnarité et les niveaux d'énergie. Remarquablement la formule $E_n = -Ry\frac{Z^2}{n^2}$ reste inchangée mais il y a un gros bonus! Pour le même "nombre quantique" n caractérisant le niveau d'énergie il y a plusieurs solutions possibles à l'équation et donc plusieurs fonctions d'onde ou états possibles. Cela signifie qu'il y a plusieurs distributions de probabilités possibles pour l'électron autour du noyau. On dit que les niveaux d'énergie sont dégénérés. Nous n'allons pas discuter ceci en détail ici, mais c'est ce qui permet d'expliquer plusieurs propriétés du tableau périodique. Ainsi l'équation de Schrödinger est à la base de la chimie.

Nous donnons ici une dérivation très heuristique de l'équation de Schrödinger. Pour une particule d'impulsion p et d'énergie E nous associons la fonction d'onde

$$\psi(z,t) = A\,\exp\{\frac{i}{\hbar}(pz - Et)\}. \tag{1.39}$$

Si la particule est libre $E = \frac{p^2}{2m}$. Supposons que la particule soit soumise à un potentiel $V(z)$. Alors la mécanique classique nous dit que $E = \frac{p^2}{2m} + V(z)$ et il est tentant de remplacer E par cette expression dans l'onde plane. Ceci n'est pas vraiment permis, mais on peut considérer que c'est une bonne approximation si $V(z)$ varie très lentement sur une échelle plus grande que $\lambda = \frac{h}{p}$:

$$\psi(z,t) \simeq A\,\exp\{\frac{i}{\hbar}(pz - \frac{p^2}{2m} + V(z))\}. \tag{1.40}$$

Il est facile de vérifier que cette fonction satisfait

$$i\hbar\frac{\partial\psi(z,t)}{\partial t} = -\frac{\hbar^2}{2m}\,\frac{d^2}{dz^2}\psi(z,t) + V(z)\psi(z,t) \tag{1.41}$$

Cette équation est en fait exacte (pour des particules non-relativistes). C'est l'équation dérivée par Schrödinger en 1926. A trois dimensions elle se généralise aisément,

$$i\hbar\frac{\partial\psi(\vec{r},t)}{\partial t} = -\frac{\hbar^2}{2m}\,\Delta\psi(\vec{r},t) + V(\vec{r})\psi(\vec{r},t) \tag{1.42}$$

Avec $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$ l'opérateur Laplacien. Dans le cas de l'atome, l'électron orbite autour du noyau de charge Ze et on prend $V(\vec{r}) = -k\frac{Ze^2}{r}$.

Pour calculer les niveaux d'énergie on suppose qu'il existe des solutions stationnaires. Ces solutions sont de la forme

$$\psi(\vec{r}, t) = \phi(\vec{r}) \exp\{-\frac{i}{\hbar} Et\} \tag{1.43}$$

Les noeuds de $\psi(\vec{r}, t)$ sont ceux de $\phi(\vec{r})$ qui ne dépend pas du temps. De plus la densité de probabilité de trouver la particule en $\vec{r}$ est $|\psi(\vec{r}, t)|^2 = |\phi(\vec{r})|^2$ qui ne dépend pas du temps.

Pour un atome, si on suppose que l'électron est lié au noyau on cherchera des solutions telles que $\phi(\vec{r}) \to 0$ pour $|\vec{r}| \to +\infty$. On se représente souvent $|\phi(\vec{r})|^2$ comme une sorte de "nuage électronique" autour du noyau.

En remplaçant l'ansatz ci-dessus dans l'équation de Schrödinger on trouve

$$\left(-\frac{\hbar^2}{2m}\Delta + V(\vec{r})\right) \phi(\vec{r}) = E\, \phi(\vec{r}). \tag{1.44}$$

Cette équation est une équation aux valeurs propres pour l'opérateur linéaire

$$H = -\frac{\hbar^2}{2m}\Delta + V(\vec{r}). \tag{1.45}$$

La fonction d'onde stationnaire $\phi(\vec{r})$ est le "vecteur propre" et E la "valeur propre" associée. L'opérateur linéaire peut être vu comme une matrice infinie (celle-ci est infini car l'espace des fonctions $\phi(\vec{r})$ est un espace vectoriel de dimension infinie). Cette matrice infinie ou opérateur est l'Hamiltonien quantique du système. Les valeurs propres donnent les niveaux d'énergie. Pour l'Hydrogène $V(\vec{r}) = -k\frac{e^2}{r}$ le calcul de Schroedinger donne $E_n = -\frac{R_y}{n^2}$. Remarquablement c'est le même résultat que la théorie de Bohr. Cette coincidence est limitée au cas spaecial de l'atome d'Hydrogène et pour d'autres systèmes il faut recourir à l'équation fondamentale de Schroedinger.

1.9 Le principe de correspondance - complément facultatif

Reprenons le problème de la particule dans un champ de forces décrit par un potentiel $V(\vec{r})$. Classiquement l'énergie est calculée comme $E = \frac{\vec{p}^2}{2m} + V(\vec{r})$. L'équation de Schroedinger nous enseigne que les niveaux d'énergie discrets sont donnés par les valeurs propres de $H = -\frac{\hbar^2}{2m}\Delta + V(\vec{r})$. Nous voyons que l'on

peut obtenir l'Hamiltonien quantique en remplaçant $V(\vec{r})$ par $V(\vec{r})$ et $\frac{\vec{p}^2}{m}$ par $-\frac{\hbar^2}{2m}\Delta$. Ceci est une expression du "principe de correspondance".

Le principe de correspondance est un ensemble de règles qui permet de déduire la forme des lois quantiques à partir des lois classiques. Grâce à ce principe on peut remplacer n'importe quelle observable classique $A(\vec{r},\vec{p})$ (c.à.d. une fonction de la position et de l'impulsion) par un opérateur ou une matrice (infinie) notée $\hat{A}$. La règle de base est donnée par la correspondance

$$\begin{cases} \vec{r} & \longrightarrow & \vec{r} = (x,y,z) \\ \vec{p} & \longrightarrow & i\hbar\vec{\nabla} = \left(i\hbar\frac{\partial}{\partial x}, i\hbar\frac{\partial}{\partial y}, i\hbar\frac{\partial}{\partial z}\right). \end{cases} \tag{1.46}$$

Par exemple, $\frac{\vec{p}^2}{2m} = \frac{p_x^2}{2m} + \frac{p_y^2}{2m} + \frac{p_z^2}{2m}$ devient $-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} - \frac{\hbar^2}{2m}\frac{\partial^2}{\partial y^2} - \frac{\hbar^2}{2m}\frac{\partial^2}{\partial z^2} = -\frac{\hbar^2}{2m}\Delta$. L'application de la règle ci-dessus donne bien

$$\frac{p^2}{2m} + V(\vec{r}) \to -\frac{\hbar^2}{2m}\Delta + V(\vec{r}). \tag{1.47}$$

Ce principe souffre d'une ambiguité qui est la suivante. Classiquement $xp_x - p_x x = 0$ car on multiplie des nombres. Néanmoins on peut montrer que

$$-x\left(i\hbar\frac{\partial}{\partial x}\right) + \left(i\hbar\frac{\partial}{\partial x}\right)x = i\hbar \tag{1.48}$$

En effet:

$$-x\left(i\hbar\frac{\partial}{\partial x}\phi(x)\right) + i\hbar\frac{\partial}{\partial x}\left(x\phi(x)\right) = -xi\hbar\phi'(x) + i\hbar x\phi'(x) + i\hbar\phi(x) \tag{1.49}$$

$$= i\hbar\phi(x). \tag{1.50}$$

Ainsi x et $p_x \equiv -i\hbar\frac{\partial}{\partial x}$ ne commutent pas en mécanique quantique (il faut y penser comme à des opérateurs ou des matrices). La quantité

$$xp_x - p_x x \equiv [x, p_x] \tag{1.51}$$

s'appelle le commutateur de x et p_x. La relation

$$[x, p_x] = i\hbar, \qquad \text{(idem pour } y, p_y \text{ et } z, p_z) \tag{1.52}$$

s'appelle la relation de commutation canonique. En fait cette relation est intimement liée au principe d'incertitude $\delta x \delta p \geq \frac{\hbar}{2}$.

Le principe de correspondance ne précise pas quel est l'ordre correct des produits entre x et p pour des observables $A(x,p)$ qui contiennent des termes mixtes. Le bon choix est guidé par des considérations physiques spécifiques au problème donné.

2 Degrés de Liberté Discrets: Polarisation et Spin

2.1 Polarisation des ondes électromagnétiques

Les équations de Maxwell dans le vide possèdent des solutions qui sont des ondes planes. Pour une onde plane se propageant dans la direction z les champs électriques $\vec{E}$ et magnétiques $\vec{B}$ sont perpendiculaires à la direction de propagation

$$\vec{E} = \mathrm{Re}\left\{\vec{E_0}\, e^{i(kz-\omega t)}\right\} \qquad \text{et} \qquad \vec{B} = \frac{1}{c}\hat{z} \times \vec{E} \tag{2.1}$$

avec $k = \dfrac{2\pi}{\lambda}$, $\omega = 2\pi\nu$ et $\lambda\nu = c$ la vitesse de la lumière. Il suffit de considérer le vecteur $\vec{E}$ car $\vec{B}$ est automatiquement $\perp$ à $\vec{E}$.

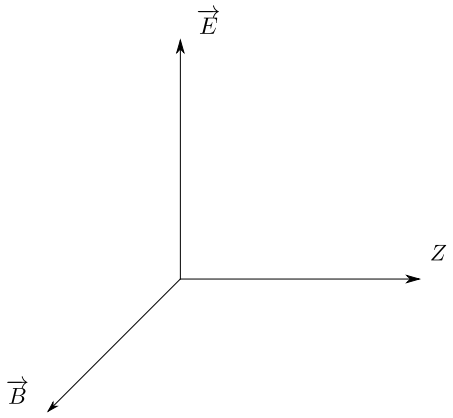


Figure 2.1 Directions des champs électrique et magnétique

En général $\vec{E_0} = \vec{E_0}\left((\cos\theta)e^{i\delta_x}; (\sin\theta)e^{i\delta_y}; 0\right)$. L'orientation de $\vec{E}$ dans le plan $\perp$ à z s'appelle la polarisation de l'onde. On peut toujours poser $\delta_x = 0$ et garder le paramètre δ_y ouvert (cela revient à changer l'origine du temps). Il est possible

de montrer que pour z fixé le vecteur champ électrique $\vec{E} = (E_x, E_y, 0)$ trace une ellipse en fonction du temps dans le plan $xy \perp z$. Ici nous allons considérer uniquement quelques cas particuliers importants.

Soit $\delta_x = 0$ et $\delta_y = 0$. On a pour $z = 0$

$$\vec{E} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \cdot \cos(\omega t) \tag{2.2}$$

Puisque $\dfrac{E_y}{E_x} = \tan\theta$, le champ électrique oscille le long de la direction θ ou bien $-\theta$. C'est ce que l'on appelle la polarisation linéaire le long de θ.

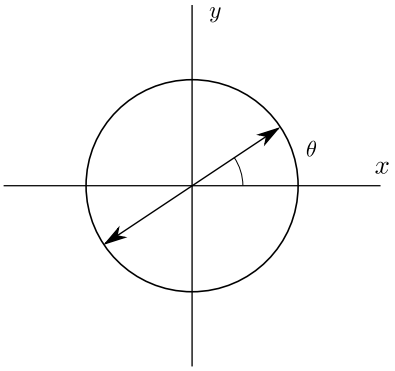


Figure 2.2 Polarisation linéaire le long de θ

Considérons le cas $\theta = \dfrac{\pi}{4}$ et $\delta_x = 0$ avec $\delta_y = \dfrac{\pi}{2}$ ou bien $\delta_y = -\dfrac{\pi}{2}$. Le champ électrique devient :

$$\vec{E} = E_0 \frac{\sqrt{2}}{2} \begin{pmatrix} \cos(\omega t) \\ \pm \sin(\omega t) \\ 0 \end{pmatrix} \tag{2.3}$$

Cette fois $E_y^2 + E_x^2 = E_0^2$ donc le champ électrique effectue un mouvement circulaire droite ou gauche.

Le cas général (θ, δ_y) quelconque (on peut toujours prendre $\delta_x = 0$) est celui de la polarisation elliptique : le champ électrique parcourt une ellipse dans la direction droite ou gauche. Les cas linéaires et circulaires sont des formes dégénérées

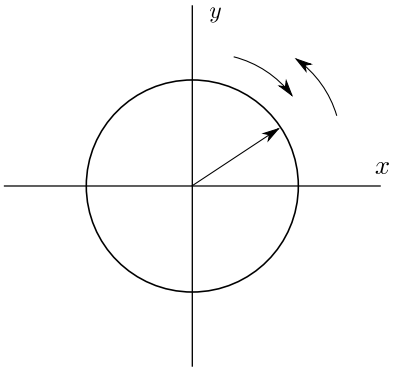


Figure 2.3 Mouvement circulaire du champ électrique

de l'ellipse. On peut mettre en évidence la polarisation des ondes électromagnétiques grâce à des filtres. Par exemple un "**polarisateur linéaire**" permet de sélectionner la composante du champ électrique dans une direction donnée disons θ. Symboliquement :

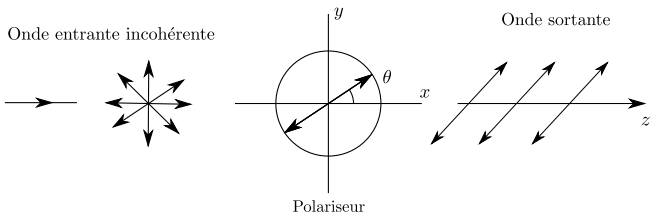


Figure 2.4 Polariseur linéaire

Le champ électrique sortant est simplement la composante du champ entrant le long de θ. Donc le champ de l'onde sortante est ici (en $z = 0$ mettons)

$$\vec{E} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \tag{2.4}$$

On peut placer un "deuxième filtre en série" le long de la direction α. Celui-ci s'appelle un "analyseur" car il sert à analyser la polarisation de l'onde.

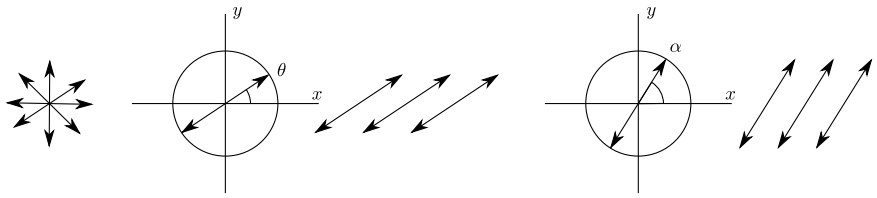


Figure 2.5 Analyseur

L'onde transmise par l'analyseur possède un champ électrique dans la direction α. Celui-ci est simplement la composante du champ entrant dans la direction α.

$$\vec{E} = E_0 \cos(\alpha - \theta) \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ 0 \end{pmatrix} \tag{2.5}$$

Ici l'amplitude est obtenue en faisant le produit scalaire

$$(\cos\alpha, \sin\alpha) \cdot \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \cos\alpha\cos\theta + \sin\alpha\sin\theta = \cos(\alpha - \theta) \tag{2.6}$$

L'intensité de l'onde avant l'analyseur (et après le premier polariseur) est $\sim E_0^2$ alors que celle après l'analyseur est $\sim E_0^2(\cos(\alpha-\theta))^2$. Le rapport des intensités transmises et incidentes est donc

$$\cos^2(\alpha - \theta) \tag{2.7}$$

C'est la loi de **Malus**.

2.2 Polarisation du photon

Le photon possède un "degré de liberté interne" qui ressemble à la polarisation du champ électrique. C'est ce qui s'appelle la "polarisation du photon".

Au premier chapitre nous avons introduit le concept de fonction d'onde. En particulier l'onde plane associée à une particule libre se propageant dans la direction $z\psi(z,t) = A\, e^{i(kz-\omega t)}$. Pour des photons cette fonction d'onde est à valeurs vectorielles tout comme le champ électrique :

$$A\, e^{i(kz-\omega t)} \begin{pmatrix} \cos\theta \\ (\sin\theta)e^{i\phi} \\ 0 \end{pmatrix} \tag{2.8}$$

Ici nous avons posé $\delta_x = 0$ et $\delta_y = \phi$ comme il est usuellement fait pour des photons.

Le choix $\phi = 0, \pi$ correspond à un photon avec la polarisation linéaire dans la direction θ ou $\theta_\perp$ et $\theta = \frac{\pi}{4}$ et $\phi = \frac{\pi}{2}$ ou $-\frac{\pi}{2}$ correspond à un photon avec polarisation circulaire droite ou gauche.

En notation de Dirac l'état général d'un photon libre est :

$$e^{i\omega t}|k\rangle \otimes (\cos\theta|x\rangle + (\sin\theta)e^{i\phi}|y\rangle). \tag{2.9}$$

La correspondance avec la notation usuelle est

$$|k\rangle \leftrightarrow e^{ikz}; \qquad |x\rangle \leftrightarrow \begin{pmatrix}1\\0\\0\end{pmatrix} \text{ et } \qquad |y\rangle \leftrightarrow \begin{pmatrix}0\\1\\0\end{pmatrix} \tag{2.10}$$

En fait on posera $|x\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ et $|y\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ et l'on fera abstraction de la composante z qui est toujours nulle.

Dans ce chapitre nous nous intéressons uniquement au "degré de liberté de polarisation" du photon:

$$|\theta,\phi\rangle = \cos\theta|x\rangle + (\sin\theta)e^{i\phi}|y\rangle = \begin{pmatrix}cos\theta\\(\sin\theta)e^{i\phi}\end{pmatrix} \tag{2.11}$$

et laissons tomber le "degré de liberté orbital" $|k\rangle$. Nous laissons aussi tomber la dépendance temporelle $e^{i\omega t}$. Ces vecteurs forment l'espace vectoriel $\mathbb{C}^2$ et satisfont $\langle\theta,\phi|\theta,\phi\rangle = 1$. Pour vérifier cela on utilise

$$\langle\theta,\phi| = \cos\theta\langle x| + e^{-i\phi}\sin\theta\langle y| \tag{2.12}$$

et

$$\langle x|x\rangle = \langle y|y\rangle = 1, \qquad \langle x|y\rangle = \langle y|x\rangle = 0. \tag{2.13}$$

On peut aussi le vérifier en composante grâce à :

$$\langle x| = (1,0) \qquad , \qquad \langle y| = (0,1) \tag{2.14}$$

et

$$\langle\theta,\phi| = (\cos\theta, e^{-i\phi}\sin\theta). \tag{2.15}$$

Les états de polarisation linéaire:

$$\begin{cases} |\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle = \begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix} \\ |\theta_\perp\rangle = \cos\theta_\perp|x\rangle + \sin\theta_\perp|y\rangle = \sin\theta|x\rangle - \cos\theta|y\rangle = \begin{pmatrix}\sin\theta\\ -\cos\theta\end{pmatrix} \end{cases} \tag{2.16}$$

forment une base orthonormée pour $\mathbb{C}^2$. Ceci est aussi le cas pour les deux états de polarisation circulaire:

$$\begin{cases} |R\rangle = |x\rangle + i|y\rangle = \begin{pmatrix}1\\ i\end{pmatrix} \\ |L\rangle = |x\rangle - i|y\rangle = \begin{pmatrix}1\\ -i\end{pmatrix} \end{cases} \tag{2.17}$$

2.3 Expériences sur la polarisation des photons

Nous allons maintenant considérer une source de photons uniques préparés dans l'état $|\theta\rangle$ de polarisation linéaire. Cela peut par exemple être réalisé grâce à une source de très basse intensité devant laquelle on place un filtre polarisateur placé selon l'angle θ.

Photodétection après un analyseur

Les photons uniques sont envoyés sur un analyseur α puis enregistrés dans un photodétecteur D.

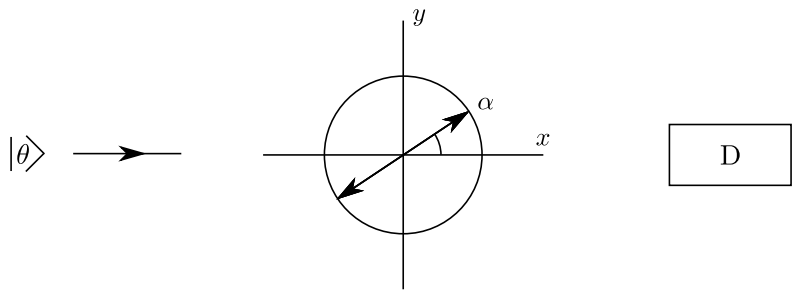


Figure 2.6 Analyseur et photodétecteur

L'observation expérimentale est la suivante: le photodétecteur enregistre 1 ou 0 photons. C'est-à-dire que le photon traverse l'analyseur α ou bien est absorbé

et ne parvient pas à D. Si l'expérience est répétée plusieurs fois on observe une séquence aléatoire

$$100101110010101 \tag{2.18}$$

et il n'est pas possible de prévoir si le photon traverse ou non l'analyseur. La deuxième observation expérimentale est la fréquence empirique des 1: la probabilité empirique de voir un photon dans le photodétecteur D est

$$\cos^2(\theta - \alpha). \tag{2.19}$$

Ces observations peuvent être expliquées très facilement grâce à la règle de Born introduite au chapitre 1. L'état du photon avant l'analyseur est $|\theta\rangle$. Le système analyseur + détecteur joue ici le rôle d'appareil de mesure. Si le détecteur enregistre un photon c'est que celui-ci est observé dans l'état $|\alpha\rangle$ (il a traversé l'analyseur). La probabilité de transition est :

$$\text{Prob}\ (|\theta\rangle \to |\alpha\rangle) = |\langle\alpha|\theta\rangle|^2 \tag{2.20}$$

en vertu de la règle de Born, il est facile de voir que

$$\begin{aligned}\langle\alpha|\theta\rangle &= (\cos\alpha\langle x| + \sin\alpha\langle y|)(\cos\theta|x\rangle + \sin\theta|y\rangle) \\ &= \cos\alpha\cdot\cos\theta + \sin\alpha\cdot\sin\theta \\ &= \cos(\alpha-\theta).\end{aligned} \tag{2.21}$$

Décomposition par une lame biréfringente

Une lame biréfringente décompose la lumière en deux parties. L'une possède une polarisation verticale et l'autre une polarisation horizontale.

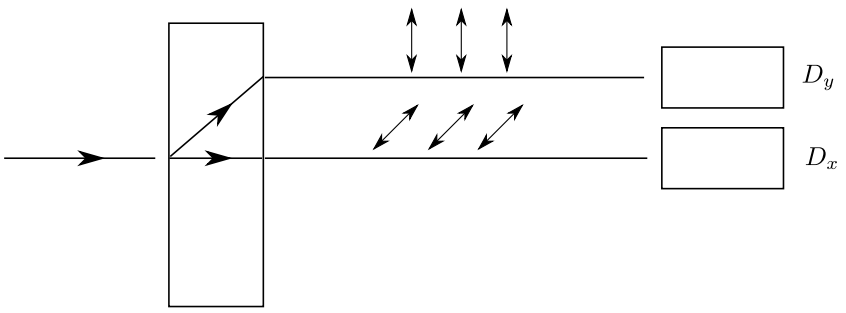


Figure 2.7 Lame biréfringente

Pour une onde avec champ électrique

$$\vec{E} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \mathrm{Re}\left\{ e^{i(kz-\omega t)} \right\} \tag{2.22}$$

On obtient deux ondes après la lame biréfringente :

$$E_y = E_0 \begin{pmatrix} 0 \\ \sin\theta \\ 0 \end{pmatrix} \mathrm{Re}\left\{ e^{i(kz-\omega t)} \right\} \tag{2.23}$$

et

$$E_x = E_0 \begin{pmatrix} \cos\theta \\ 0 \\ 0 \end{pmatrix} \mathrm{Re}\left\{ e^{i(kz-\omega t)} \right\} \tag{2.24}$$

L'intensité mesurée dans les deux détecteurs (divisée par l'intensité incidente) est pour $D_y \sim \sin^2\theta$ et pour $D_x \sim \cos^2\theta$. La somme des intensités est égale à l'intensité totale incidente.

Que se passe-t-il si on envoie des photons uniques? On observe que D_x ou D_y enregistre un photon; ces événéments sont exclusifs. Si la séquence des enregistrements pour D_x est:

$$1010011010101, \tag{2.25}$$

pour D_y elle est:

$$0101100101010. \tag{2.26}$$

Ces séquences sont complémentaires mais aléatoires. on peut seulement connaître la statistique des 1 et 0. La probabilité empirique d'observer 1 dans D_x est $\cos^2\theta$ et elle est $\sin^2\theta$ pour D_y.

L'interprétation quantique de ce résultat est la suivante. Avant la lame biréfringente l'état du photon est $|\theta\rangle$. Après la lame biréfringente l'état orbital est différent (il existe "deux chemins possibles") mais l'état de polarisation est toujours $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$. La probabilité d'enregistrer un photon dans D_x est la probabilité d'observer une polarisation $|x\rangle$:

$$\mathrm{Prob}\ (|\theta\rangle \to |x\rangle) = |\langle x|\theta\rangle|^2 = \cos^2\theta \tag{2.27}$$

La probabilité d'enregistrer un photon dans D_y est la probabilité d'observer une polarisation $|y\rangle$:

$$\text{Prob}\ (|\theta\rangle \to |y\rangle) = |\langle y|\theta\rangle|^2 = \sin^2\theta \tag{2.28}$$

Décomposition - Recombinaison

Cette fois-ci au lieu d'observer les photons juste après la lame biréfringente, on recombine l'onde (ou les photons) grâce à une lame symmétrique. Ensuite on analyse les photons avec le système analyseur α + détecteur.

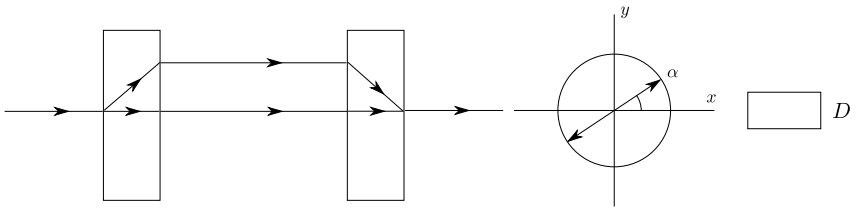


Figure 2.8 Décomposition et recombinaison

Si l'expérience est faite avec une onde électromagnétique, celle-ci est d'abord décomposée entre les lames, puis recomposée. Après la deuxième lame le champ électrique est donné par la superposition

$$E_x + E_y = \text{Re}\left\{e^{i(kz-\omega t)}\right\} E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} \tag{2.29}$$

Après l'analyseur l'intensité enregistrée dans le détecteur sera donc $\cos^2(\theta - \alpha)$.

Avec des photons uniques on enregistre ou non un photon dans le détecteur. A nouveau lorsque l'expérience est répétée on obtient une suite aléatoire de 1 et 0. La fréquence empirique des 1 est $\cos^2(\theta - \alpha)$.

Ce résultat est "évident" si l'on accepte l'interprétation quantique. En effet après la seconde lame biréfringente l'état du photon est $|\theta\rangle$ (à nouveau!). La probabilité que celui-ci soit détecté par l'appareil $\alpha + D$ est donc

$$\text{Prob}(|\theta\rangle \to |\alpha\rangle) = |\langle\alpha|\theta\rangle|^2 = \cos^2(\alpha - \theta). \tag{2.30}$$

Il est instructif de faire un calcul "purement classique" en supposant que les photons se comportent comme des particules classiques ayant des trajectoires et des polarisations uniques bien définies. Nous allons voir que le résultat n'est pas en accord avec l'expérience.

Si la "particule" est classique elle suit le chemin supérieur avec probabilité

$\sin^2\theta$ et le chemin inférieur avec probabilité $\cos^2\theta$. Quand elle suit le chemin supérieur sa polarisation est "y" et la probabilité de détection après l'analyseur doit être $\cos^2(\frac{\pi}{2}-\alpha) = \sin^2\alpha$. Quand elle suit le chemin inférieur sa polarisation est "x" et la probabilité de détection après l'analyseur doit être $\cos^2(0-\alpha) = \cos^2\alpha$. Ainsi:

$$\begin{aligned}\text{Prob(détection)} &= \text{Prob(détection} \mid \text{chemin sup)Prob(chemin sup)} \\ &+ \text{Prob(détection} \mid \text{chemin inf)Prob(chemin inf)} \\ &= \sin^2\theta\sin^2\alpha + \cos^2\theta\cos^2\alpha \\ &\neq (\cos(\theta-\alpha))^2. \end{aligned} \tag{2.31}$$

La différence entre le résultat d'une interprétation classique et le (vrai) résultat quantique est égale à $2\sin\theta\sin\alpha\cos\theta\cos\alpha$. En effet:

$$\begin{aligned}\cos^2(\theta-\alpha) &= (\cos\theta\cos\alpha + \sin\theta\sin\alpha)^2 \\ &= \cos^2\theta\cos^2\alpha + \sin^2\theta\sin^2\alpha + 2\cos\theta\sin\theta\cos\alpha\sin\alpha. \end{aligned} \tag{2.32}$$

La situation est en fait très similaire à l'expérience des fentes de Young. Le terme qui est absent dans le calcul classique est un terme d'interférence entre les "deux chemins possibles": avant d'être observés dans le photodétecteur les photons ont un comportement ondulatoire et on ne peut pas leur associer des trajectoires et des états de polarisations "x" et "y" bien définis. Leur état est $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$ tant qu'ils ne sont pas détectés.

2.4 Observables associées à la polarisation

Reprenons l'expérience de photodétection avec le système Analyseur + Détecteur.

Nous avons vu que si le photon entrant est dans l'état $|\theta\rangle$ la Prob(clic) = $\cos^2(\theta-\alpha) = |\langle\alpha|\theta\rangle|^2$ et la Prob(pas de clic) = $\sin^2(\theta-\alpha) = |\langle\alpha_\perp|\theta\rangle|^2$. Le clic détecte une transition $|\theta\rangle \to |\alpha\rangle$ et l'absence de clic détecte une transition $|\theta\rangle \to |\alpha_\perp\rangle$. Nous pouvons enregistrer les résultats de l'expérience dans une variable (aléatoire) $p_\alpha = +1$ (clic) et $p_\alpha = -1$ (pas de clic). La valeur moyenne de cette variable aléatoire est

$$\mathbb{E}[p_\alpha] = (+1)|\langle\alpha|\theta\rangle|^2 + (-1)|\langle\alpha_\perp|\theta\rangle|^2 \tag{2.33}$$

.

Plus généralement si l'état entrant dans le système Analyseur + Détecteur est $|\psi\rangle$ un état de $\mathbb{C}^2 = \left\{ \begin{pmatrix} a \\ b \end{pmatrix};\ a \text{ et } b \in \mathbb{C} \text{ et } |a|^2 + |b|^2 = 1 \right\}$ on a:

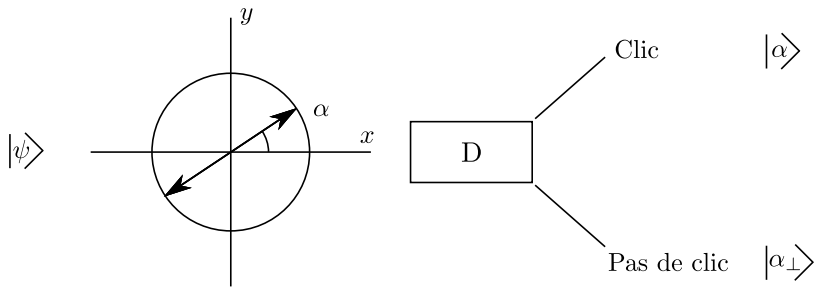


Figure 2.9 Expérience de photodétection

$$\mathbb{E}[p_\alpha] = (+1)|\langle\alpha|\psi\rangle|^2 + (-1)|\langle\alpha_\perp|\psi\rangle|^2 \tag{2.34}$$

Cette expression peut se mettre sous la forme

$$\mathbb{E}[p_\alpha] = (+1)\langle\psi|\alpha\rangle\langle\alpha|\psi\rangle + (-1)\langle\psi|\alpha_\perp\rangle\langle\alpha_\perp|\psi\rangle \tag{2.35}$$

(Ici on utilise $\overline{\langle\alpha|\psi\rangle} = \langle\psi|\alpha\rangle$ qui est une propriété du produit scalaire). En d'autres termes

$$\begin{aligned}\mathbb{E}[p_\alpha] &= \langle\psi|\ (|\alpha\rangle\langle\alpha| - |\alpha_\perp\rangle\langle\alpha_\perp|)\ |\psi\rangle \\ &\equiv \langle\psi|P_\alpha|\psi\rangle\end{aligned} \tag{2.36}$$

où on a **défini** "l'observable polarisation"

$$P_\alpha = (+1)|\alpha\rangle\langle\alpha| + (-1)|\alpha_\perp\rangle\langle\alpha_\perp|. \tag{2.37}$$

Avant de discuter la signification physique de P_α, nous discutons sa signification mathématique. Ici $|\alpha\rangle\langle\alpha|$ est un ket fois un bras c'est-à-dire un vecteur fois son transposé: ceci est un projecteur sur le vecteur $|\alpha\rangle$. De même $|\alpha_\perp\rangle\langle\alpha_\perp|$ est un projecteur sur $|\alpha_\perp\rangle$. Ces projecteurs ne sont rien d'autre que des matrices:

$$|\alpha\rangle\langle\alpha| = \begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}\begin{pmatrix}\cos\alpha & \sin\alpha\end{pmatrix} = \begin{pmatrix}\cos^2\alpha & \cos\alpha\sin\alpha\\ \sin\alpha\cos\alpha & \sin^2\alpha\end{pmatrix} \tag{2.38}$$

$$|\alpha_\perp\rangle\langle\alpha_\perp| = \begin{pmatrix}-\sin\alpha\\ \cos\alpha\end{pmatrix}\begin{pmatrix}-\sin\alpha & \cos\alpha\end{pmatrix} = \begin{pmatrix}\sin^2\alpha & -\cos\alpha\sin\alpha\\ -\sin\alpha\cos\alpha & \cos^2\alpha\end{pmatrix} \tag{2.39}$$

et donc

$$P_\alpha = \begin{pmatrix}\cos(2\alpha) & \sin(2\alpha)\\ \sin(2\alpha) & -\cos(2\alpha)\end{pmatrix} \tag{2.40}$$

On peut vérifier que cette matrice possède les valeures propres ± 1 associées aux vecteurs propres $|\alpha\rangle = \begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}$ et $|\alpha_\perp\rangle = \begin{pmatrix}-\sin\alpha\\ \cos\alpha\end{pmatrix}$. C'est-à-dire:

$$P_\alpha|\alpha\rangle = (+1)|\alpha\rangle \tag{2.41}$$

$$P_\alpha|\alpha_\perp\rangle = (-1)|\alpha_\perp\rangle \tag{2.42}$$

En fait il est très instructif de faire cette vérification en notation de Dirac plutôt qu'en travaillant avec le tableau matriciel.

$$\begin{aligned} P_\alpha|\alpha\rangle &= \left(|\alpha\rangle\langle\alpha| - |\alpha_\perp\rangle\langle\alpha_\perp|\right)|\alpha\rangle \\ &= |\alpha\rangle\underbrace{\langle\alpha|\alpha\rangle}_{1} - |\alpha_\perp\rangle\underbrace{\langle\alpha_\perp|\alpha\rangle}_{0} \\ &= |\alpha\rangle \end{aligned} \tag{2.43}$$

$$\begin{aligned} P_\alpha|\alpha\rangle &= \left(|\alpha\rangle\langle\alpha| - |\alpha_\perp\rangle\langle\alpha_\perp|\right)|\alpha_\perp\rangle \\ &= |\alpha\rangle\underbrace{\langle\alpha|\alpha_\perp\rangle}_{0} - |\alpha_\perp\rangle\underbrace{\langle\alpha_\perp|\alpha_\perp\rangle}_{1} \\ &= -|\alpha_\perp\rangle \end{aligned} \tag{2.44}$$

Quelle est l'interprétation physique de la matrice ou "observable" P_α? Cette matrice caractérise la quantité mesurée, ici "la polarisation du photon dans les directions $(\alpha, \alpha_\perp)$". L'appareil qui sert à mesurer cette quantité est l'Analyseur + Détecteur. Le résultat de la mesure est donné par les valeurs propres et vecteurs

propres de la matrice. Ici il y a deux résultats possibles (+1, $|\alpha\rangle$) et (-1, $|\alpha_\perp\rangle$). La probabilité d'obtenir (+1, $|\alpha\rangle$) est $|\langle\alpha|\psi\rangle|^2$ ou bien $\langle\psi|\alpha\rangle\langle\alpha|\psi\rangle$. La probabilité d'obtenir (-1, $|\alpha_\perp\rangle$) est $|\langle\alpha_\perp|\psi\rangle|^2$ ou bien $\langle\psi|\alpha_\perp\rangle\langle\alpha_\perp|\psi\rangle$. La valeur moyenne de "l'observable" est $\langle\psi|P_\alpha|\psi\rangle$.

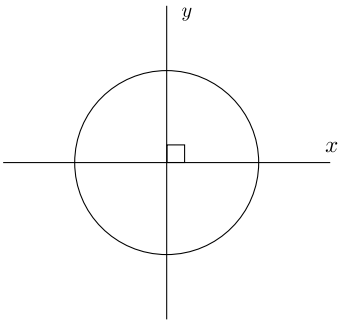
Si l'analyseur fait un angle β (avec x) et non pas α, l'appareil de mesure est différent. L'observable mesurée est alors aussi différente, notamment $P_\beta = |\beta\rangle\langle\beta| - |\beta_\perp\rangle\langle\beta_\perp|$.

Il existe trois observables qui jouent un rôle privilégié et que nous rencontrerons plus tard souvent.

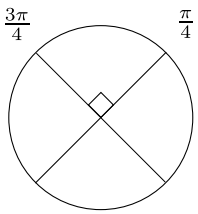
Si $\alpha = 0$, l'analyseur mesure la polarisation dans les directions x et y et

$$P_{\alpha=0} = |x\rangle\langle x| - |y\rangle\langle y| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.45}$$

On symbolise souvent cet analyseur ou cet "appareil de mesure" par



Si $\alpha = \dfrac{\pi}{4}$, l'analyseur mesure la polarisation dans les directions $\dfrac{\pi}{4}$ et $\dfrac{3\pi}{4}$ et cet appareil de mesure est souvent symbolisé par



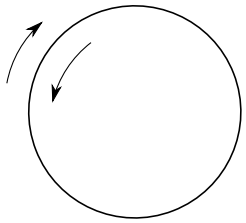
L'observable correspondant est:

$$P_{\alpha=\frac{\pi}{4}} = |\frac{\pi}{4}\rangle\langle\frac{\pi}{4}| - |\frac{3\pi}{4}\rangle\langle\frac{3\pi}{4}| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.46}$$

Si on utilise un analyseur qui mesure la polarisation circulaire l'observable correspondante est:

$$P_{\text{circ}} = |R\rangle\langle R| - |L\rangle\langle L| = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}. \tag{2.47}$$

Le symbole pour cet analyseur est



Il est instructif de vérifier cette identité en utilisant

$$|R\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \qquad \langle R| = \frac{1}{\sqrt{2}} \begin{pmatrix} 1, & -i \end{pmatrix} \tag{2.48}$$

$$|L\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \qquad \langle L| = \frac{1}{\sqrt{2}} \begin{pmatrix} 1, & i \end{pmatrix} \tag{2.49}$$

Nous verrons dans les axiomes de la MQ qu'une quantité mesurable est toujours représentée par une matrice hermitienne. Les résultats d'une mesure de cette quantité sont les valeurs propres et vecteurs propres de cette matrice. Si λ_i et $|v_i\rangle$ sont valeur propre et vecteur propre de la matrice, la règle de Born stipule que

$$\text{Prob(observer } \lambda_i \text{ et } |v_i\rangle) \ = |\langle v_i|\psi\rangle|^2 \tag{2.50}$$

quand $|\psi\rangle$ est l'état initial avant la mesure.

2.5 Moments magnétiques classiques

Dans les quelques paragraphes qui suivent nous discutons un autre type de degré de liberté classique: le spin 1/2. Tout d'abord nous devons faire quelques rappels sur la notion de moment magnétique classique.

Considérons une boucle de courant plongée dans un champ magnétique uniforme (voir figure).

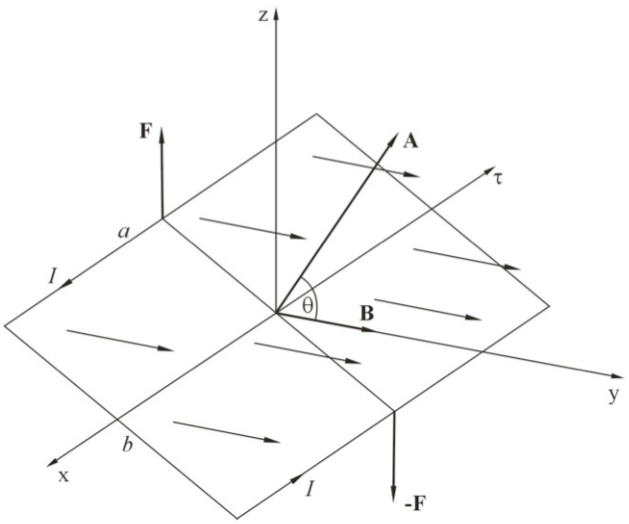


Figure 2.10 Boucle rectangulaire porteuse d'un courant électrique et plongée dans un champ magnétique uniforme

Si cette boucle est traversée par un courant la force de Laplace qui s'exerce sur les sections du fil aura tendance à ramener la boucle dans la position d'équilibre. Cette position d'équilibre correspond à la boucle de courant $\perp$ à $\vec{B}$ de façon à ce que les forces de Laplace s'équilibrent. L'origine microscopique de la force de Laplace est en fait la force de Lorentz. Pour une particule de charge q, de vitesse $\vec{v}$, dans un champ magnétique $\vec{B}$, la force de Lorentz qui s'exerce sur cette particule est (produit vectoriel ici): $\vec{F} = q\vec{v} \times \vec{B}$. Si δq est la quantité de charge traversant une section du fil pendant un temps δt le terme la force s'exercant sur une longueur $\delta\vec{l}$ du fil est $\delta\vec{F} = \delta q \frac{\delta\vec{l}}{\delta t} \times \vec{B} = I\delta\vec{l} \times \vec{B}$. Cette dernière expression est celle de la force de Laplace. On peut calculer le travail total de la force de Laplace s'exercant sur la boucle de courant et en déduire que celle-ci possède une énergie potentielle dans le champ magnétique. La boucle est à l'équilibre lorsque cette énergie est minimale (cas ou la boucle est $\perp$ au champ). Un calcul (que nous omettons ici) montre que cette énergie potentielle est donnée par

$$E = -\vec{M} \cdot \vec{B} \tag{2.51}$$

où $\vec{M}$ est le *moment magnétique* associé à la boucle de courant $\vec{M} = I\vec{S}$, avec $\vec{S}$ le vecteur unité perpendiculaire à la surface de longueur égale à la surface. On peut comprendre intuitivement cette formule en remarquant que (force de Laplace)$\times$(distance) possède les mêmes unités. Ce calcul montre aussi que l'on peut associer un moment magnétique à une charge q en rotation autour de la boucle de courant

$$\vec{M} = \frac{q}{2}\vec{r} \times \vec{v} = \frac{q}{2m}\vec{L} \tag{2.52}$$

où $\vec{L} = \vec{r} \times \vec{p}$ est le moment cinétique. L'énergie est minimale lorsque le moment cinétique $\vec{L}$ ou bien le moment magnétique $\vec{M}$ pointent dans la direction du champ $\vec{B}$; et est maximale lorsque $\vec{L}$ ou $\vec{M}$ pointent dans la direction opposée au champ.

Il existe aussi d'autres types de "moments magnétiques" dans la nature qui ne sont pas associés au mouvement de charges, mais sont "intrinsèques aux particules". Par exemple l'électron, le proton, le neutron (et par conséquent les noyaux atomiques) possèdent des moments magnétiques intrinsèques. Tout se passe comme si ces particules étaient des petites toupies en rotation sur elles memes ce qui produit des boucles de courant. Néanmoins cette image classique est trop naive et n'est finalement pas très utile pour comprendre le formalisme necessaire à la description des moments magnétiques intrinsèques. Nous allons voir que les formules $E = -\vec{M} \cdot \vec{B}$ et $\vec{M} \sim \frac{q}{2m}\vec{L}$ sont toujours valables sauf que $\vec{L}$ et $\vec{M}$ sont des vecteurs dont les composantes sont des matrices! Dans ce contexte le vecteur (à composantes matricielles) $\vec{L}$ s'appelle le *spin* (et on utilise plutot la notation $\vec{S}$ à la place de $\vec{L}$).

2.6 L'expérience de Stern-Gerlach

L'expérience célèbre de Stern et Gerlach mis en évidence le "moment magnétique intrinsèque" de l'électron. A ce moment magnétique intrinsèque est associé un "moment cinétique intrinsèque" que l'on appelle le spin.

L'expérience consiste à préparer un faisceau d'atomes d'Argent qui sortent d'un four et à faire passer ce faisceau à travers un champ magnétique possédant un gradient dans la direction z.

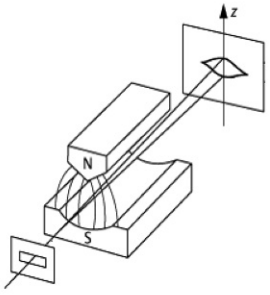


Figure 2.11 Expérience de Stern et Gerlach

Lorsque les particules passent à travers l'aimant le faisceau est séparé en deux et on observe deux taches séparées sur l'écran.

Ce résultat expérimental est étonnant à plusieurs titres. Tout d'abord l'atome d'Argent est neutre si bien que la force de Lorentz ne devrait pas affecter la

trajectoire du faisceau. On peut très bien imaginer que, bien que neutres, les atomes d'Argent possèdent un moment magnétique $\vec{M}$ non nul. Alors la force qui s'exerce entre eux vaut $\vec{\nabla}(\vec{M} \cdot B) = \vec{M} \cdot \vec{\nabla} B$ et on conçoit que le faisceau soit dévié. Mais on s'attendrait à ce que à la sortie du four $\vec{M}$ soit "incohérent" et pointe dans des directions aléatoires. Puisque $\vec{M} \cdot \vec{\nabla} B = M_z(\vec{\nabla} B)_z$ et M_z est continu (prend des valeurs aléatoires) on s'attendrait à observer une tache plus ou moins uniforme étalée sur l'écran. Mais l'observation consiste en deux petites taches séparées (le long de l'axe z). *Cela indique qu'en fait M_z prend deux valeurs possibles.*

Cette *quantification du moment magnétique* ne peut pas être expliquée par la physique classique. Les électrons de l'atome d'Argent (et tous les électrons dans la nature) possèdent un moment magnétique intrinsèque qui n'a rien à voir avec leur mouvement orbital. Ce moment magnétique intrinsèque prend deux valeurs possibles. Pour les atomes d'Argent le nombre total d'électrons est impair et il se trouve que les moments magnétiques intrinsèques des électrons se compensent deux à deux sauf pour l'électron de la couche atomique externe de l'atome d'Argent. Cet électron sur la couche atomique externe confère à l'atome un moment magnétique quantifié prenant deux valeurs possibles.

Dans le paragraphe suivant nous discutons le moment magnétique intrinsèque et le spin de l'électron.

2.7 Spin $\frac{1}{2}$ et moments magnétiques quantiques

Les particules élémentaires possèdent un moment cinétique intrinsèque appelé "spin" et un moment magnétique intrinsèque associé. Le spin est une sorte d'analogue du moment cinétique $\vec{L}$. Néanmoins il serait trop naïf de considérer la particule (ici l'électron) comme une boule minuscule tournant sur elle-même. Rappelons nous que nous avons déjà abandonné la notion de trajectoire bien définie.

Le "vecteur" associé au spin est noté $\vec{S}$. De façon analogue à $\vec{L} = (L_x, L_y, L_z)$ il possède trois composantes (S_x, S_y, S_z). L'unité de $\vec{L}$ est "quantité de mouvement $\times$ position" = "J·s" = unité de $\hbar$. Pour cette raison on posera

$$\vec{S} = \frac{\hbar}{2}\vec{\sigma} \tag{2.53}$$

où $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ sont des composantes sans dimension. Comme nous allons le voir ces composantes sont chacunes des matrices: en effet le spin (tout comme $\vec{L} = \vec{r} \times \vec{p} \to \vec{r} \times \frac{\hbar}{i}\vec{\nabla}$) est une observable donc une matrice en MQ.

Le moment magnétique associé au spin est

$$\vec{M} = \gamma \vec{S} \tag{2.54}$$

tout comme $\vec{M} = \frac{q}{2m}\vec{L}$ pour une particule de charge q (et masse m). Ici γ est une constante qui dépend aussi de q et m; pour une particule chargée telle que l'électron $\gamma = g\frac{q}{2m}$ avec $g \approx 2.002...$; pour le proton $g \approx 5$.

L'énergie associée à l'interaction entre le moment magnétique et le champ magnétique est comme dans le cas classique donnée par

$$-\vec{M} \cdot \vec{B} = -\gamma \frac{\hbar}{2} \vec{\sigma} \cdot \vec{B} \tag{2.55}$$

Comme pour toutes les observables en MQ, nous allons voir que cette quantité est une matrice (qui s'appelle l'Hamiltonien du spin dans le champ $\vec{B}$).

En bloquant un des deux faisceaux dans l'appareil de Stern-Gerlach on peut fabriquer un **filtre** qui est l'analogue des filtres polariseurs et/ou analyseurs. Ce filtre sélectionne un des deux états possibles pour les particules de "spin 1/2". On peut alors procéder à des expériences similaires à celles faites avec les photons.

Cela mène alors à la conclusion suivante. Pour des particules telles que l'électron, les matrices $\sigma_x, \sigma_y, \sigma_z$ sont des matrices 2×2 similaires aux observables de polarisation linéaires et circulaires:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad \sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}; \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.56}$$

Lors de l'expérience de Stern-Gerlach on mesure en fait la composante z du spin. Le résultat de la mesure donne deux valeurs possibles correspondant aux valeurs propres de $M_z = \gamma \frac{\hbar}{2}\sigma_z$. Ces deux valeurs propres sont égales à ± 1 multipliées par la constante $\gamma \frac{\hbar}{2}$. Les vecteurs propres correspondants sont

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv |\uparrow\rangle \qquad \text{et} \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |\downarrow\rangle \tag{2.57}$$

et ce sont les deux états possibles obtenus lors de la mesure de σ_z. On peut vérifier qu'en notation de Dirac:

$$\sigma_z = (+1)|\uparrow\rangle\langle\uparrow| + (-1)|\downarrow\rangle\langle\downarrow| \tag{2.58}$$

$$= \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.59}$$

Si on tourne l'appareil le long de l'axe x, on mesure l'observable σ_x ou le moment magnétique $M_x = \gamma \frac{\hbar}{2}\sigma_x$. Les valeurs propres sont à nouveau ± 1 et les états propres correspondants sont

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \equiv |+\rangle \tag{2.60}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle) \equiv |-\rangle \tag{2.61}$$

En notation de Dirac

$$\sigma_x = (+1)|+\rangle\langle+| + (-1)|-\rangle\langle-| \tag{2.62}$$

De même on a pour σ_y les valeurs propres ± 1 avec les états propres

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\downarrow\rangle) \equiv |\circlearrowleft\rangle \tag{2.63}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle - i|\downarrow\rangle) \equiv |\circlearrowright\rangle \tag{2.64}$$

et

$$\sigma_y = (+1)|\circlearrowleft\rangle\langle\circlearrowleft| + (-1)|\circlearrowright\rangle\langle\circlearrowright| \tag{2.65}$$

2.8 L'espace de Hilbert du spin $\frac{1}{2}$

Nous avons vu que les photons possèdent un degré de liberté de polarisation. Les états quantiques possibles de la polarisation du photon sont des vecteurs de l'espace de Hilbert $\mathbb{C}^2 = \left\{ \begin{pmatrix}a\\b\end{pmatrix};\ a \text{ et } b \in \mathbb{C} \text{ et } |a|^2 + |b|^2 = 1 \right\}$.

Un état général peut s'écrire en notation de Dirac $a|x\rangle + b|y\rangle$ où $|x\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ et $|y\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. De plus pour les photons une paramétrisation naturelle qui est analogue à la paramétrisation de la polarisation du champ électrique consiste à prendre $a = \cos\theta$ et $b = (\sin\theta)e^{i\phi}$. Ainsi les états de polarisation du photon sont en général

$$|\theta, \phi\rangle = \cos\theta|x\rangle + e^{i\phi}\sin\theta|y\rangle \tag{2.66}$$

avec $0 \leq \theta \leq \pi$ et $0 \leq \phi \leq 2\pi$.

Les particules de "spin 1/2" possèdent un degré de liberté interne analogue à la polarisation pour un photon. Des exemples de particules possédant un spin 1/2 sont l'électron, le proton, le neutron,... Les noyaux atomiques possèdent un

spin total qui est la somme des spins des protons et neutrons. Souvent ceux-ci se compensent entre eux et si le nombre de protons et neutrons est impair le spin résultant du noyau classique est à nouveau de "type 1/2". Comme nous l'avons vu ce degré de liberté peut prendre essentiellement deux valeurs lors d'une mesure (par exemple avec un appareillage de Stern-Gerlach).

Ainsi l'espace des vecteurs d'état du spin 1/2 est à nouveau l'espace à deux dimensions $\mathbb{C}^2 = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} ;\ a \text{ et } b \in \mathbb{C} \text{ et } |a|^2 + |b|^2 = 1 \right\}$. Cette fois on préfère noter $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\uparrow\rangle$ et $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\downarrow\rangle$.
La paramétrisation naturelle est presque la même que pour les photons. Un état général de spin est

$$|\theta, \phi\rangle = \cos(\frac{\theta}{2})|\uparrow\rangle + e^{i\phi} \sin(\frac{\theta}{2})|\downarrow\rangle. \tag{2.67}$$

avec $0 \leq \theta \leq \pi$ et $0 \leq \phi \leq 2\pi$. La présence de $\frac{\theta}{2}$ au lieu de θ signifie entre autres que

$$|\theta = 0, \phi = 0\rangle = |\uparrow\rangle \quad \text{et} \quad |\theta = \pi, \phi = 0\rangle = |\downarrow\rangle. \tag{2.68}$$

Cette paramétrisation est naturelle car si on renverse le champ magnétique dans l'appareil de Stern-Gerlach on échange les deux taches sur l'écran. Renverser le champ magnétique revient à faire $\theta : 0 \to \pi$ et échanger les deux taches correspond à $|\uparrow\rangle \to |\downarrow\rangle$.

Notez que pour les photons, tourner un polariseur d'un angle π ne change pas la direction de polarisation. De même pour les photons $|\theta = 0, \phi = 0\rangle = |x\rangle$ et $|\theta = \pi, \phi = 0\rangle = -|x\rangle$ qui est équivalent à $|x\rangle$ (à une phase $e^{i\pi}$ près).

2.9 Notion de Bit Quantique

Nous avons vu que "l'espace de Hilbert" à deux dimensions

$$\mathbb{C}^2 = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} ;\ a \text{ et } b \in \mathbb{C} \right\} \tag{2.69}$$

muni du produit scalaire

$$\begin{pmatrix} \overline{c} & \overline{d} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \overline{c}\, a + \overline{d}\, b \tag{2.70}$$

intervient dans la description de deux systèmes physiques: la polarisation du photon et le spin 1/2 (de l'électron ou de certains noyaux atomiques).

Les degrés de libertés décrits par cet espace de Hilbert s'appelle aussi des

systèmes à deux niveaux. La nature nous offre toute une variété de systèmes à deux niveaux décrits par l'espace des états $\mathbb{C}^2$. Parfois $\mathbb{C}^2$ est une description exacte du système comme c'est le cas pour la polarisation du photon et le spin de l'électron (ou du proton, neutron, noyaux atomiques). Parfois c'est une description approximative qui consiste à retenir la partie importante des degrés de liberté plus compliqués. C'est le cas par exemple avec la molécule de Benzène C_6H_6. Dans des conditions normales (température ambiante) la molécule de Benzène existe dans l' état $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$ de superposition des deux états de base de la figure ci-dessous. C'est l'état stable d'énergie la plus basse. Quand la molécule absorbe de la lumière ultraviolette (photons) elle peut passer dans l'état excité d'énergie plus élevée $\frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$. Les états de base de la figure ne sont pas stable: on peut se faire l'image d'une molécule qui résonne ou oscille entre ces deux états.

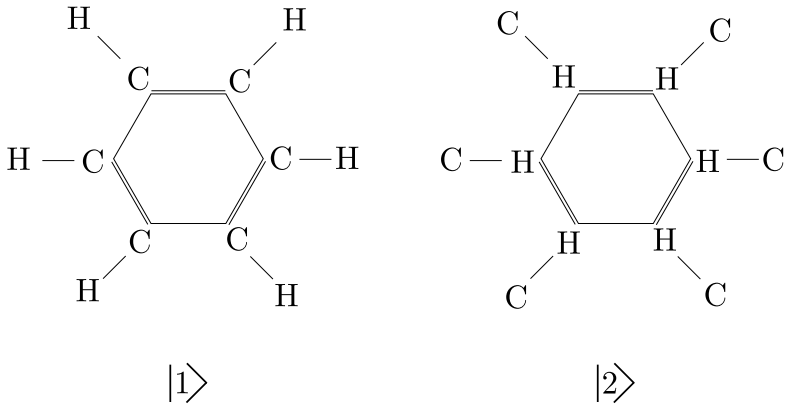


Figure 2.12 Molécule de Benzène. Les barres représentent les liaisons chimiques impliquant une paire d'électrons. Les doubles barres sont des doubles liaisons impliquant deux paires. L'état stable du Benzène est $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$.

On pourrait donner beaucoup d'autres exemples de systèmes à deux niveaux dans la nature, dans le domaine de la chimie, de la physique moléculaire ou atomique, de la physique nucléaire et des particules élémentaires.

Le bit quantique est simplement l'abstraction de la notion de système à deux niveaux du contexte physique détaillé. Un bit quantique est un état du type

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{2.71}$$

où $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $a, b \in \mathbb{C}$ avec $|a|^2 + |b|^2 = 1$.

On adopte souvent (par convention) la convention relative au spin 1/2 c.à.d.

$a = \cos\frac{\theta}{2}$ et $b = e^{i\phi}\sin\frac{\theta}{2}$ (mais pour la notion abstraite du bit quantique cela n'est pas obligatoire).

Le bit quantique est un degré de liberté qui possède une nature duale. Il est discret dans la mesure ou l'espace $\mathbb{C}^2$ possède la dimension 2 et les résultats de mesure sont binaires. Il est continu dans la mesure ou α et β sont des nombres complexes continus. Nous reviendrons sur ces considérations.

2.10 La sphère de Bloch

L'espace de Hilbert du bit quantique $\mathbb{C}^2$, t.q. $|\psi\rangle = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$ est abstrait. La sphère de Bloch est une représentation géométrique très utile. Celle-ci est basée sur la paramétrisation

$$|\psi\rangle = |\theta, \phi\rangle = (\cos\frac{\theta}{2})|0\rangle + e^{i\phi}(\sin\frac{\theta}{2})|1\rangle \tag{2.72}$$

ou

$$|\psi\rangle = |\theta, \phi\rangle = (\cos\frac{\theta}{2})|\uparrow\rangle + e^{i\phi}(\sin\frac{\theta}{2})|\downarrow\rangle \tag{2.73}$$

On représente $|\theta, \phi\rangle$ par un vecteur unité sur une sphère où θ est l'angle par rapport à z et ϕ est l'angle par rapport à x dans le plan (x, y). Ici θ et ϕ ne sont rien d'autres que les coordonnées sphériques.

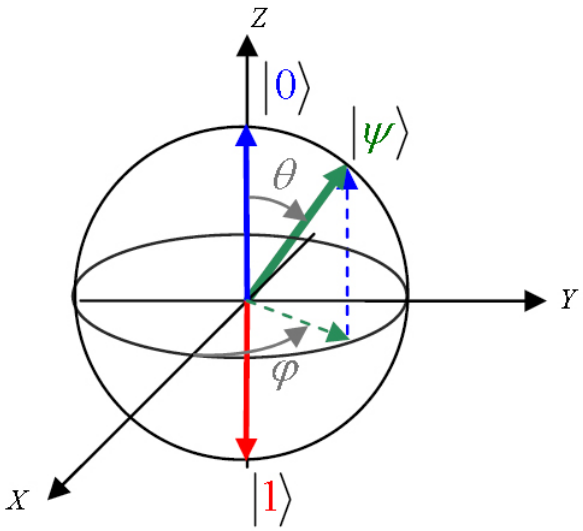


Figure 2.13 La sphère de Bloch

Les états des trois bases orthonormées ci-dessous

$$\{|\uparrow\rangle \quad ; \quad |\downarrow\rangle\} \quad \text{ou bien} \quad \{|0\rangle \quad ; \quad |1\rangle\} \tag{2.74}$$

$$\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) = |+\rangle \quad ; \quad \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle) \ = |-\rangle\} \tag{2.75}$$

$$\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\downarrow\rangle) = |\circlearrowleft\rangle \quad ; \quad \frac{1}{\sqrt{2}}(|\uparrow\rangle - i|\downarrow\rangle) = |\circlearrowright\rangle\} \tag{2.76}$$

sont représentés sur la sphère de Bloch.

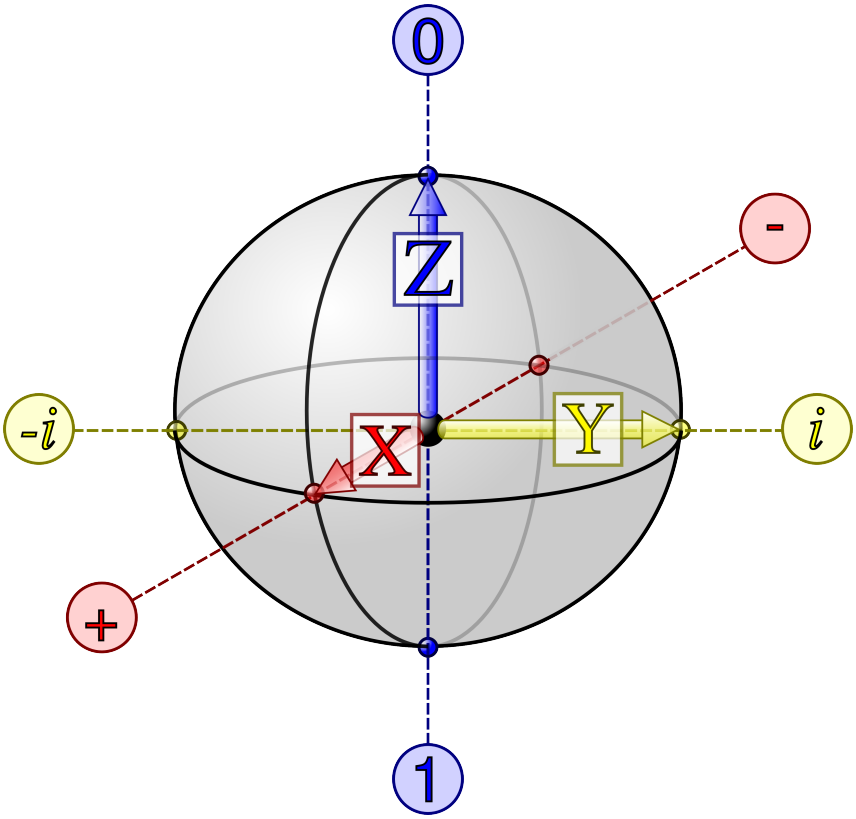


Figure 2.14 Représentation des trois états de bases orthonormées sur la sphère de Bloch, ici $|i\rangle = |\circlearrowleft\rangle$ et $|-i\rangle = |\circlearrowright\rangle$, $|0\rangle = |\uparrow\rangle$ et $|1\rangle = |\downarrow\rangle$

Ces trois bases s'appellent, pour des raisons évidentes les bases Z, X et Y en information quantique. Elles correspondent aux bases des états propres des trois matrices de Pauli du spin σ_z, σ_x et σ_y. Ces matrices sont aussi appelées souvent Z, X et Y.

3 Principes de la Mécanique Quantique

La physique moderne est fondée sur la Mécanique Quantique. Cette théorie a été élaborée suite à plusieurs expériences [p.ex: raies spectrales, corps noir, effet photoélectrique, effet Compton, diffraction des electrons sur les cristaux, physique atomique, expérience de Stern Gerlach etc...] et travaux des pères fondateurs [p.ex: Planck sur le corps noir 1900, Einstein sur le photon 1905, Bohr sur l'atome 1913, De Broglie sur la fonction d'onde 1924, Schroedinger sur l'évolution de la fonction d'onde 1926, Born sur l'interpretation de la fonction d'onde 1926, Heisenberg sur la formulation algebrique 1925, Dirac sur la mecanique quantique relativiste 1930, etc...]. Un bref aperçu de quelques-uns de ces sujets a été donné au premier chapitre.

En 1930 les grands principes physiques de la mécanique quantique étaient essentiellement connus. Leur formulation mathématique précise et un cadre cohérent fut donné par Dirac et von Neumann. Leurs livres "Principles of Quantum Mechanics" (Dirac 1930) et "Mathematische Grundlagen der Quantenmechanik" (von Neumann 1932) jouèrent un role fondamental. Aujourd'hui même, les grands principes sont inchangés, et combinés avec les principes de la relativité décrivent avec un succès une gamme impressionante de phénomènes sur les échelles de distances, d'énergies et de températures associées à la physique de la matière condensée, atomique et moléculaire, nucléaire, sub-nucléaire. Malheureusement on ne sait toujours pas combiner de facon cohérente la théorie classique de la gravitation avec la mécanique quantique, et dans ce domaine il n'existe aussi pas d'expériences pouvant guider les physiciens (car la force de gravité est en fait trés faible).

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

3.1 Algèbre linéaire en notation de Dirac

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

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

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

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

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

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

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

et

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

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

Nous aurons besoin de la notion de produit tensoriel. Soit $\mathcal{H}_1$ et $\mathcal{H}_2$ deux espaces de Hilbert avec deux bases finies. Soit $|i\rangle_1$, $i = 1, ..., n_1$ la première base de $\dim \mathcal{H}_1 = n_1$ et $|j\rangle_2$, $j = 1, ..., n_2$ celle de $\dim \mathcal{H}_2 = n_2$. Nous pouvons former "l'espace produit"

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

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

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

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

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

Un vecteur général de l'espace produit est

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

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

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

.

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

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

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

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

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

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

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

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

Inégalités de Cauchy-Schwarz. Comme d'habitude:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On définit aussi le *commutateur*

$$[A, B] = AB - BA$$

et l'anticommutateur

$$\{A, B\} = AB + BA$$

Projecteurs en notation de Dirac. L'opération linéaire

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

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

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

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

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

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

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

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

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

$$A = \sum_n a_n P_n$$

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

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

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

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

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

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

Nous écrirons souvent la décomposition spectrale sous la forme

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

3.2 Principes de la mécanique quantique

Dans ce paragraphe nous expliquons les 5 grands principes de la MQ:

- les systèmes isolés sont décrits par *des vecteurs (kets) états d'un espace de Hilbert*,
- le vecteur d'état *évolue dans le temps de facon unitaire*,

- les *observables* sont décrites par des *matrices hermitiennes*,
- l'opération de mesure est un processus distinct de l'évolution temporelle: c'est une *projection aléatoire*,
- on peut *composer* des systèmes: leur espace d'Hilbert est un espace produit (tensoriel).

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

Exemple 4.

- La polarization du photon est décrite par $\mathcal{H} = \mathbf{C}^2$. Les vecteurs d'état de $\mathbf{C}^2$ sont $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. Un état de polarisation linéaire $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, un état de polarisation circulaire $|\tilde{\theta}\rangle = \cos\theta|0\rangle + i\sin\theta|1\rangle$, et un état général
$$\cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$$
- Le spin $\frac{1}{2}$ (de l'électron par exemple) est décrit par le même espace d'Hilbert. La paramétrisation naturelle est
$$\cos\frac{\theta}{2}|0\rangle + e^{i\delta}\sin\frac{\theta}{2}|1\rangle$$
La sphère de Bloch est une représentation géométrique naturelle de l'espace de Hilbert de ces états.
- Pour une particule dans $\mathbf{R}^3$ on a $\mathcal{H} = L^2(\mathbf{R}^3)$. Les vecteurs d'états sont les fonctions d'ondes normalisées $\int d^3\vec{x}|\psi(\vec{x})|^2 = 1$.

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

L'évolution unitaire forme un groupe (ou plutot la représentation du groupe des translations temporelles) au sens suivant:
$$U_{t=0} = I, \qquad U_{t_1}U_{t_2} = U_{t_1+t_2}$$

La MQ nous indique comment calculer U_t pour un système donné: il faut résoudre *l'équation de Schroedinger*. En information quantique nous ne nous interessons pas (en général) à cette équation. On suppose (de facon optimiste) qu'un ingénieur ou un physicien saura construire un appareil (appelé circuit quantique) qui réalise l'opération unitaire U_t voulue. L'opération voulue sera spécifiée par l'algorithme quantique. Nous reviendrons sur ce point plus tard dans le cours.

Exemple 5. Un mirroir semi-transparent decompose un rayon incident en rayon réfléchi et rayon transmis. Soit $\mathcal{H} = \mathbf{C}^2$ l'espace de Hilbert avec la base $|T\rangle$, $|R\rangle$.

Le mirroir semi-transparent agit de facon unitaire

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

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

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

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

Principe 3: quantités observables. En mécanique quantique une quantité observable (énergie, moment magnétique moment, position, impulsion, vitesse,...) est représentée par une matrice hermitienne.

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

Exemple 6.

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

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

  cette observable est la matrice hermitienne $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (dans la base $|x\rangle$, $|y\rangle$).
- Toute observable (matrice hermitienne) de $\mathcal{H} = \mathbf{C}^2$ peut être représentée par une matrice 2×2

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

  ou en notation de Dirac

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

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

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

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

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

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

et

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

Principe 4: postulat de la mesure. Soit un système préparé dans l'état $|\psi\rangle$. On veut mesurer une observable du système grâce â un appareil. L'appareil est modélisé par un ensemble de projecteur orthogonaux $\{P_n\}$ satisfaisant $\sum_n P_n = I$. Une mesure *projette*[1] l'état ψ du système qui devient juste après la mesure

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

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

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

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

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

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

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

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

Conséquence importante concernant la mesure des observables. Ce point est fondamental car ce sont les observables que l'on mesure dans une expérience. L'appareil de mesure modélisé par un ensemble de projecteurs $\{P_n\}$ permet de mesurer toutes les observables de la forme $A = \sum_j a_j P_j$. Une mesure donne $|\psi\rangle \to |\phi_n\rangle$ pour un certain n. Puisque $A|\phi_n\rangle = a_n|\phi_n\rangle$, la valeur de A donnée par la mesure est précisément a_n.

La valeur moyenne des mesures de A si l'état du système est $|\psi\rangle$

$$\sum_j a_j\langle\psi|P_j|\psi\rangle = \langle\psi|A|\psi\rangle$$

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

et la variance

$$\sum_j a_j^2 \langle\psi|P_j|\psi\rangle - (\sum_j a_j \langle\psi|P_j|\psi\rangle)^2 = \langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2$$

En pratique on utilise le membre de droite de ces formules pour calculer les valeurs moyennes et variances.

Après une mesure le vecteur d'état est réduit à$|\psi\rangle \to |\phi_n\rangle$, pour un certain n, et la valeur moyenne dans le nouvel état (i.e $|\phi_n\rangle$) devient a_n, et la variance devient nulle.

De plus on ne peut mesurer avec le même appareil que des observables ayant les mêmes projecteurs propres. En particulier la mesure simultanée (avec un même appareil) n'a de sens que si les observables ont les mêmes projecteurs et vecteurs propres. Elles peuvent avoir des valeurs propres différentes mais doivent commuter. Nous reviendrons sur ce point lorque nous formulerons l'inégalité de Heisenberg.

Exemple 7: measure de polarisation du photon. Pour mesurer l'observable

$$\mathcal{P} = |x\rangle\langle x| - |y\rangle\langle y|$$

on utilise l'appareil constitué d'un analyseur orienté le long de x et un détecteur. Cet appareil est la réalisation physique de la base de mesure $\{|x\rangle, |y\rangle\}$. Si le photon traverse l'analyseur l'état juste après la mesure est $|x\rangle$, et si le photon est absorbé l'état juste après la mesure est $|y\rangle$. Les probabilités associées sont

$$\text{Prob(resultat } +1) = |\langle x|\psi\rangle|^2, \ \text{Prob(resultat } -1) = |\langle y|\psi\rangle|^2$$

Si la préparation initiale de la polarisation des photons est $|\psi\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$ ces probabilités sont simplement $\cos^2\theta$ et $\sin^2\theta$. Supposons que l'analyseur soit tourné d'un angle γ. cela signifie que l'on mesure l'observable

$$\mathcal{P} = |\gamma\rangle\langle\gamma| - |\gamma_\perp\rangle\langle\gamma_\perp|$$

Les probabilités associée à cette mesure sont

$$\text{Prob(resultat } +1) = |\langle\gamma|\psi\rangle|^2 = \cos^2(\theta - \gamma)$$

$$\text{Prob(resultat } -1) = |\langle\gamma_\perp|\psi\rangle|^2 = \sin^2(\theta - \gamma)$$

Finalement notons que dans le premier cas l'observable mesurée est la matrice

$$\mathcal{P} = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

et dans le second cas

$$\mathcal{P} = \begin{pmatrix} \cos 2\gamma & \sin 2\gamma \\ \sin 2\gamma & -\cos 2\gamma \end{pmatrix} = (\cos 2\gamma)Z + (\sin 2\gamma)X$$

.

Principe d'incertitude Prenons un système dans l'état $|\psi\rangle$ et considérons deux observables A et B. Elles ont chacune une représentation spectrale

$$A = \sum_j a_j P_j, \quad B = \sum_j b_j Q_j$$

Comme expliqué précédemment dans l'état $|\psi\rangle$, chaque observable possède la valeur moyenne $\langle\psi|A|\psi\rangle$, $\langle\psi|B|\psi\rangle$ et l'écart type $\Delta A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2}$, $\Delta B = \sqrt{\langle\psi|B^2|\psi\rangle - \langle\psi|B|\psi\rangle^2}$. La relation ou inégalité d'incertitude de Heisenberg stipule

$$\Delta A \cdot \Delta B \geq \frac{1}{2}\langle\psi|[A,B]|\psi\rangle$$

L'interprétation de cette inégalité est la suivante. Si $[A,B] \neq 0$ il n'est pas possible de mesurer A et B simultanément avec precision infinie. Si $\Delta A = 0$ alors $\Delta B = \infty$. L'exemple le plus frappant est $A = x$ (position) and $B = p = \frac{\hbar}{i}\frac{\partial}{\partial x}$ (impulsion ou quantité de mouvement). dans ce cas $\Delta x \Delta p \geq \frac{h}{4\pi}$ et on ne peut pas mesurer avec précsion infinie position et impulsion de la particule: ce n'est pas une limitation technologique mais une limitation imposée par les lois de la nature.

Si $[A,B] = 0$ il existe une base commune de l'espace de Hilbert dans laquelle A et B sont toutes deux diagonales. En mesurant dans cette base, le postulat de la mesure indique que les observables peuvent être mesurées avec précision infinie. Il n'y a pas de contradiction avec le principe d'incertitude car le menbre de droite de l'inégalité de Heisenberg s'annule quand $[A,B] = 0$.

Principe 5: sytèmes quantiques composés. Prenons deux systèmes $\mathcal{A}$ et $\mathcal{B}$ avec espaces de Hilbert $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$. L'espace de Hilbert du système composé $\mathcal{AB}$ est donné par le produit tensoriel

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

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

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

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

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

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

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

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

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

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

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

3.3 Etats produit et état intriqués

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

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

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

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

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

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

et

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

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

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

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

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

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

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

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

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

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

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

3.4 Impossibilité de "cloner" un état quantique

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

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

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

La machine produit la sortie:

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

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

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

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

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

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

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

En prenant l'hermitien conjugué de la deuxième équation

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

En prenant le produit scalaire avec la première équation

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

ce qui implique

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

donc

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

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

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

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

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

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

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

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

ceci implique

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

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

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

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

Part II

II. Information et Calcul Quantiques

4 Cryptographie Quantique

Une des premières applications de la MQ à la théorie de l'information quantique est le protocole inventé par Bennett et Brassard en 1984 pour la distribution d'une clé secrète entre deux acteurs distants (Alice et Bob). Depuis d'autres protocoles ont vu le jour et une nouvelle discipline "la cryptographie quantique" a émergée. A proprement parler, comme nous le verrons il ne s'agit pas vraiment de cryptographie, mais plutot de méthodes de génération de clé secrète commune.

L'idée générales du protocole BB84 est la suivante. Alice envoie une suite de bits classiques - la clé secrète - à Bob en utilisant des qubits intermédiaires[1]. Toute tentative, de la part d'un troisième acteur (Eve) d'extraction d'information, à propos de la clé nécessite d'observer les qubits. selon les postulats de la MQ cette observation perturbe l'état des qubits. Nous verrons qu'Alice et Bob sont capables de détecter cette perturbation, et donc la présence d'Eve. Dans un tel cas de figure la communication est arrétée.

Le sujet est bien plus compliqué que le traitement exposé dans ce chapitre. En réalité le canal de communication (la fibre optique) est bruité et il n'est pas évident de distinguer les perturbations d'Eve de celles associées au bruit. D'autrepart les opérations d'Alice et Bob ne sont pas parfaites, au niveau de la préparation des états ainsi qu'au niveau de leurs mesures. La preuve mathématique de la sécurité du protocole de BB84 repose sur des hypothèses qui peuvent en pratique être violées. Néanmoins si l'on accepte certaines hypothèses, on peut démontrer la sécurité du protocole. Une telle preuve est hautement non-triviale et dépasse largement le cadre de ce cours. Nous discuterons néanmoins deux attaques simplifiées de la part d'Eve ce qui sera suffisant pour comprendre pourquoi les principes de la MQ assurent la sécurité de la clé.

La cryptographie quantique n'est pas seulement une idée théorique, c'est également un sujet véritablement expérimental. La génération de clé secrète commune à été réalisée dans les laboratoires (d'abord chez IBM en 1989, sur une distance de 32 cm!) et plus tard à l'extérieur des laboratoires sur des distances de quelques dizaines à des centaines de kilomètres (Genève, Los Alamos ...). Aujourd'hui, il existe des sociétés proposant des systèmes commerciaux [2]. Des implémentations récentes permettent la génération de clés secrètes communes sur des distance de

[1] Ici nous pouvons penser au qubit associé à la polarisation du photon; bien qu'en pratique le protocole est implémenté avec des degrés de libertés associés à la phase des photons.

[2] IdQuantique

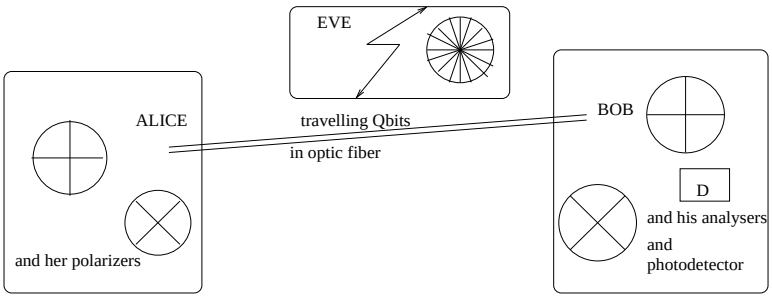


Figure 4.1 Alice et Bob génèrent une clé secrète sur le canal d'une fibre optique

100 km (resp. 250 km) à un taux de de 6000 (resp. 15) bits par seconde. Celles-ci exigent une connaissance approfondie de l'optique et ne seront pas discutées ici. Récemment, ces systèmes ont été violés en exploitant les limites physiques des photo-détecteurs du coté de Bob. En illuminant un photodétecteur de facon appropriée celui-ci fonctionne alors en mode classique et les avantages liés à la MQ sont perdus.

4.1 La génération des clés selon BB84

Le protocole comporte quatre phases essentielles: la procédure d'encodage d'Alice, la procédure de décodage de Bob, une communication publique entre les deux parties, et enfin la génération de la clé secrète commune. La figure 4.1 illustre le set-up général.

Procédure de codage d'Alice. Elle génère une suite binaire aléatoire $x_1, ..., x_n$, $x_i \in \{0, 1\}$ qu'elle garde secrète. La clé commune sera un sous-ensemble de ces bits. Elle génère également une deuxième suite binaire aléatoire $e_1, ..., e_N$, $e_i \in \{0, 1\}$ qu'elle garde secrète *pour l'instant*. Alice *encode* les bits classiques x_i en qubits comme suit:

- Pour $e_i = 0$ elle génère un qubit dans l'état $|x_i\rangle$. Concrètement, elle prépare les photons avec un polariseur dans la base Z (figure 4.2).

  $$\{|0\rangle, |1\rangle\}$$

  Pour $x_i = 0$ (resp. $x_i = 1$) le polariseur est orienté horizontalement (resp. verticalement). Ainsi les photons sont préparés dans l'état de polarisation $|0\rangle$ (resp. $|1\rangle$). Un seul photon est ensuite sélectionné dans le faisceau sortant (ce qui bien-sûr est une idéalisation).
- Pour $e_i = 1$, elle génère un qubit dans l'état[3] $H|x_i\rangle$. Concrètement, cela peut

[3] Ici H est la matrice de Hadamard $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Figure 4.2 Orientations des polariseurs pour la préparation des photons dans la base Z.

Figure 4.3 Orientations du polariseur pour la préparation des photons dans la base X.

se faire en envoyant des photons à travers un polariseur dans la base X (figure 4.3)

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

sont préparés dans un état de polarisation $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (resp. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

En résumé, Alice envoie une chaîne de qubits $|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$, $i = 1, ..., N$ par un canal (dans la pratique, une fibre optique).

Procédure de décodage de Bob . Bob génère une suite binaire aléatoire $d_1, ..., d_n$, $d_i \in \{0, 1\}$ qu'il garde secrète *pour l'instant* . Il décode les qubits reçus d'Alice comme suit:

- Si $d_i = 0$ il effectue une mesure des qubits reçus $|A_{e_i,x_i}\rangle$ dans la base Z

  $$\Big\{|0\rangle, |1\rangle\Big\}.$$

  L'état photon après la mesure

  $$|y_i\rangle \in \{|0\rangle, |1\rangle\}.$$

  est enregistré dans des bits classiques y_i. Pour ce faire, concrètement, il utilise l' appareil de mesure analyseur-détecteur décrit dans le premier chapitre: l'analyseur est placé est projeté sur $|0\rangle$; et si le détecteur ne clique pas, cela signifie que l'état photon est projeté sur $|1\rangle$. Nous soulignons que, selon le postulat de la mesure, ces résultats sont *vraiment aléatoire* . C'est uniquement Bob qui les connaît.
- Si $d_i = 1$, il effectue une mesure des qubits reçus $|A_{e_i,x_i}\rangle$ dans la base X.

  $$\Big\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle\Big\}.$$

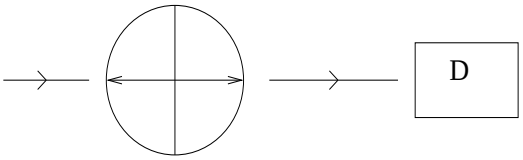


Figure 4.4 Dispositif analyseur-détecteur pour la mesure de la polarisation dans la base Z.

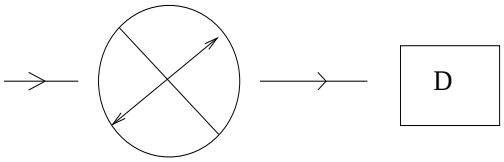


Figure 4.5 Dispositif analyseur-détecteur pour la mesure de la polarisation dans la base X.

L'état du photon après la mesure appartient à

$$H|y_i\rangle \in \Big\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \Big\}$$

Pour un état $H|y_i\rangle$, Bob enregistre le bit classique y_i . Pour ce faire, concrètement , il utilise l'appareil analyseur-détecteur décrit dans le premier chapitre : l'analyseur est tourné vers la droite (figure 4.5) à 45 degrés; si le détecteur clique cela signifie l'état des photons est projeté sur que l'état photon est projeté sur $H|1\rangle$. Nous soulignons à nouveau que, selon le postulat de la mesure ces résultats sont *vraiment aléatoire*. Seul Bob les connaît.

En résumé Bob a décodé les qubits envoyés par Alice, en une suite binaire classique $y_1, ..., y_n$. cette suite est le résultat des mesures de Bob et ne peut être prédite.

Communication Publique. Alice possède à sa disposition deux suites binaires: $e_1, ..., e_N$ utilisée pour encoder; et $x_1, ..., x_N$ qui est mappée sur les qubits. Bob aussi possède deux suites binaires: $d_1, ..., d_N$ pour choisir une base de mesure et $y_1, ..., y_N$ qui sont les résultats des mesures.

Alice et Bob communiquent $e_1, ..., e_N$ et $d_1, ..., d_N$ sur un canal public classique, et gardent les deux suites $x_1, ..., x_N$ et $y_1, ..., y_N$ secrètes. *Il importe que la communication publique ne commence qu'après la phase de mesures de Bob.* Alice et Bob peuvent déduire les informations suivantes (en fait quiconque entendant la communication publique peut déduire ces informations):

- Si $d_i = e_i$, c.a.d si ils ont utilisé la même base, alors certainement $y_i = x_i$ (on peut s'en convaincre avec quelques exemples; en fait si Bob et Alice ont utilisé la même base c'est comme s'ils vivaient dans un monde classique).

- Si $d_i \neq e_i$, c.a.d s'ils n'ont pas utilisé la même base, de véritables effets quantiques entrent en jeu quand Bob fait la mesure. Selon le postulat de la mesure $y_i \neq x_i$ avec probabilité $\frac{1}{2}$ et $y_i = x_i$ avec probabilité $\frac{1}{2}$. Prouvons le. Bob recoit le qubit

$$|A_{e_i,x_i}\rangle = H^{e_i}|x_i\rangle$$

et mesure dans la base

$$\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}.$$

Le résultat sera un des deux vecteurs de base:

$$H^{d_i}|0\rangle, \qquad \text{avec prob } |\langle 0|H^{d_i}H^{e_i}|x_i\rangle|^2$$

ou bien

$$H^{d_i}|1\rangle, \qquad \text{avec prob } |\langle 1|H^{d_i}H^{e_i}|x_i\rangle|^2.$$

Le lecteur peut vérifier que si $e_i \neq d_i$ les deux probabilités correspondantes sont égales à $\frac{1}{2}$ (et si $e_i = d_i$ elles valent 0 ou 1).

Génération de la clé commune. Bob et Alice effacent tous les bits x_i et y_i correspondant à i tel que $e_i \neq d_i$. Ils gardent les bits x_i et y_i restants indexés par i tels que $e_i = d_i$. Ils sont assurés que ces deux suites de bits sont identiques $x_i = y_i$, donc cela peut potentiellement constituer la clé secrète commune. La longueur de cette sous-suite est proche de $\frac{N}{2}$, car prob$(e_i \; neq d_i) = \frac{1}{2}$. Enfin, Alice et Bob effectuent un test de sécurité: selon la mécanique quantique on doit avoir[4]

$$\text{Prob}(x_i = y_i | e_i = d_i) = 1$$

Alice et Bob testent cette condition en échangant une petite fraction (disons $\epsilon\frac{N}{2}$) de la sous-suite commune sur le canal public. Si le test réussi, ils gardent le reste de sous suite commune: ils ont réussi à générer une clé secrète commune de longueur $(1-\epsilon)\frac{N}{2}$.

4.2 Attaques de la part d'Eve - discussion simplifiée

Nous supposons que Alice a une source de photon unique parfait, que la préparation des qubits est parfaite , qu'il n'y a pas de bruit, que les appareils de mesure de Bob sont parfaits. Dans ces conditions, lorsque Eve est absente le critère de sécurité absolue Prob$(x_i = y_i | e_i = d_i) = 1$ est satisfait.

En outre, nous supposons qu'Eve peut seulement attaquer en effectuant des opérations sur un qubit à la fois, sur les photons capturés le long de la fibre optique et qu'elle n'a pas accès aux laboratoires d'Alice et Bob. Nous supposons

[4] Sans bruit et sans la présence d'Eve.

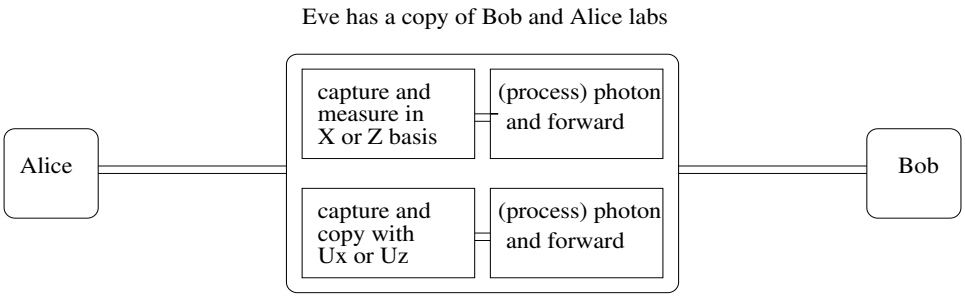


Figure 4.6 Laboratoire d'interception de photons d'Eve's sur le chemin de la fibre optique

néanmoins qu'Eve a une connaissance parfaite des orientatins X et Z des polariseurs et analyseurs d'Alice et Bob (mais pas des choix aléatoires successifs).

Nous considérons deux attaques possibles: "l'attaque basée sur une mesure" et "l'attaque basée sur des opérations unitaires ". Les deux attaques se composent de deux étapes. Premièrement Eve capture un photon, fait une mesure ou applique une opération unitaire, puis transmet le photon à Bob, ou alors lui transmet un autre photon (voir figure 4.6). Nous allons voir que les postulats de base de QM impliquent que le critère de sécurité est violé. Lorsqu'Alice et Bob constatent cette violation ils découvrent la présence d'Eve et interrompent la communication.

Attaque de type mesure. Supposons qu'Eve capture un photon dans la fibre optique. Le photon capturé est dans l'un des états

$$|A_{e_i,x_i}\rangle \in \big\{|0\rangle, |1\rangle, H|0\rangle, H|1\rangle\big\}$$

Eve effectue une mesure. Si elle utilise la base Z le résultat appartient à $\{|0\rangle, |1\rangle\}$ et elle enregistre un bit $y_i^E \in \{0,1\}$. Si elle utilise la base X son résultat est dans $\{H|0\rangle, H|1\rangle\}$ et elle enregistre le bit correspondant $y_i^E \in \{0,1\}$. Une fois qu'elle a terminé la mesure, elle envoie le photon à Bob dans le nouvel état laissé par la mesure [5]. Deux possibilités peuvent se présenter:

- Eve a utilisé la même base qu'Alice: alors $y_i^E = x_i$ et le photon est reçu par Bob dans l'état correct.
- Eve a utilisé une base différente qu'Alice: alors $y_i^E = x_i$ seulement la moitié du temps, et elle envoie à Bob le photon dans un état "correct" seulement la moitié du temps.

Voyons ce que Alice et Bob trouvent quand ils effectuent le test de sécurité. On

[5] Elle pourrait aussi envoyé un autre photon dans cet état ou un autre état mais cela ne peut pas améliorer sa performance.

note EA pour l'évènement "Eve utilise la même base que Alice".

$$\begin{aligned}\text{prob}(x_i = y_i | e_i = d_i) &= \text{prob}(x_i = y_i | e_i = d_i, EA)\text{prob}(EA) \\ &\quad + \text{prob}(x_i = y_i | e_i = d_i, \text{not } EA)\text{prob}(\text{not } EA) \\ &= 1 \cdot \text{prob}(EA) + \frac{1}{2} \cdot (1 - \text{prob}(EA)) \\ &= \frac{1}{2}(1 + \text{prob}(EA))\end{aligned}$$

où nous avons utilisé

$$\text{prob}(x_i = y_i | e_i = d_i, EA) = 1, \qquad \text{prob}(x_i = y_i | e_i = d_i, \text{not EA}) = \frac{1}{2} \quad (4.1)$$

En supposant qu' Eve n'a aucune information sur les choix de base d'Alice que nous prenons $\text{prob}(EA) = \frac{1}{2}$. Alors

$$\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}.$$

Alice et Bob savent qu'un quart des bits ne sont pas corrects même quand ils ont utilisés la même base: ils concluent qu'un espion est à l'oeuvre!

Attaque unitaire. Avec l'attaque précédente lorsqu'Eve fait une mesure, elle n'a aucune information sur la base qu'Alice a choisi. Une solution possible serait de copier les qubits $|A_{e_i,x_i}\rangle$, et laisser le photon dans l'état original arriver à Bob. La copie pourra être utilisée par eve (du moins croit-elle) après la phase de communication publique. Quand Alice et Bob entrent dans la phase de communication publique, Eve connait les choix de base de Bob. Donc pour i tel que $e_i = d_i$ elle obtient les mêmes résultat que Bob $y_i^E = y_i = x_i$. Elle partage donc le secret d'Alice et Bob.

Toutefois il y a une erreur dans le raisonnement ci-dessus. Le *théorème de non-clonage* (qui est une conséquence du postulat de l'évolution unitaire) garanti qu'il n'existe pas de machine (unitaire) telle que

$$U(|A_{e_i,x_i}\rangle \otimes |\text{blank}\rangle) = |A_{e_i,x_i}\rangle \otimes |A_{e_i,x_i}\rangle$$

Le point important est que $|A_{e_i,x_i}\rangle$ appartient à

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

qui est un ensemble d'états non-orthogonaux! (A et B ont bien travaillé leur MQ).

Eve pourrait essayer d'utiliser deux machines de copie: une pour la copie des deux états de la base Z et une autre pour la copie des deux états de la base X. Mais cette fois, elle n'a aucun moyen de savoir laquelle des deux utiliser quand un photon est capturé. Elle utilisera la mauvaise machine la moitié du temps. Une analyse similaire à la précédente montre qu'à nouveau

$$\text{prob}(x_i = y_i | e_i = d_i) = \frac{3}{4}.$$

Le critère de sécurité est violé: le quart des bits communs sont corrompus.

4.3 Le protocole de Bennet 1992

Dans BB84 Alice prépare les photons dans 4 états possibles. En fait l'analyse précédente montre que le point impiortant est que ces états ne sont pas deux à deux tous orthogonaux. Bennet inventa en 1992 un protocole qui utilise uniquement deux états non-orthogonaux: $|0\rangle$ et $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Ce protocole ainsi qu'une analyse détaillée de sa sécurité est l'objet d'un exercice.

5 Intrication Quantique

Dans ce chapitre, nous étudions la nature des corrélations présentes dans les états "intriqués". Ce sont de véritables corrélations de type quantique intrinsèquement présentes dans des systèmes quantiques à plusieurs qubits. Ces corrélations n'ont pas d'équivalent classique, en d'autres termes, elles ne peuvent pas être décrites par des distributions de probabilité classiques. On utilise le terme intrication pour désigner ce type special de corrélations dont la nature est purement quantique.

Tout d'abord nous allons discuter le prototype des états intriqués pour deux qubits: les états de Bell. Nous abordons ensuite le sujet des inégalité de Bell[1]. Ces inégalités, qui furent d'abord proposées par John Bell ($\sim$ 1964), donnent un critère d'intrication qui peut être vérifié expérimentalement. Ces expériences, qui furent d'abord réalisées par Aspect et Grangier, puis dans divers autres contextes, confirment les prédications théoriques de la MQ.

L'intrication est une ressource importante dans le traitement quantique de l'information. Elle joue un role important dans plusieurs protocoles importants pour la communication quantique. Ici nous décrirons deux applications, sous leur forme la plus simple possible: la *téléporation* et le *codage superdense*. L'intrication a aussi été utilisée dans des protocoles de cryptographie quantique (Ekert 1991; ceci pourra faire l'objet d'un exercice). Toutes ces applications ont été réalisées expérimentalement. L'intrication joue aussi un role important dans le calcul quantique que nous aborderons plus tard dans le cours.

5.1 Etats de Bell

Le prototype des états intriqués est constitué des états de Bell. Ceux-ci forment une base orthonormée de $\mathbf{C}^2 \otimes \mathbf{C}^2$ qui est un espace à 4 dimensions. Les 4 états de Bell sont

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

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) = U|01\rangle$$

[1] Nous allons en fait discuter une version plus transparente due à Clauser, Horne, Shimony, Holt (CHSH).

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) = U|10\rangle$$

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) = U|11\rangle$$

Dans ces états les deux qubits sont en quelque sorte corrélés: en effet dans l'état $|B_{00}\rangle$ les deux degrés de libertés de polarisation des deux photons sont parallèles, ou bien les deux états de spin sont parallèles. En fait il serait faux de penser que la direction (des deux spins p.ex) est up-up ou down-down. En effet le lecteur peut vérifier que

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|\gamma\gamma\rangle + |\gamma_\perp\gamma_\perp\rangle\Big) \tag{5.1}$$

où $|\gamma\rangle = \cos\gamma|0\rangle + \sin\gamma|1\rangle$. Ainsi les degres de libertés ne pointent pas dans des directions précises. Néanmoins les directions des deux degres de liberté sont corrélées.

Une paire de photons ou une paire de moments magnétiques (spins) peut être préparée dans un état de Bell. Pour cela il faut amener les deux degrés de liberté suffisamment près l'un de l'autre dans l'espace et les faire interagir. Si l'interaction est appropriée une corrélation est induite. La paire de particules peut ensuite être spatialement séparée. Si les particules ne sont pas affectées par leur environnement la corrélation des degrés de liberté de polarisation ou de spin est préservée.

Comme nous allons le voir dans ce chapitre les corrélations dont nous parlons n'ont pas d'analogue classique. On utilise le terme "intrication" pour désigner ce type special de corrélations. Les paires dans les états de Bell sont aussi appelées "paires EPR" car Einstein, Podolski et Rosen (ainsi que Schroedinger) furent parmi les premiers à attirer l'attention sur certaines propriétés en apparence paradoxales de ces états (pour les degrés de liberté de position et d'impulsion en fait).

Pour nous familiariser avec la subtilité de ces états nous commencons par discuter des scénarios de mesures possibles. Nous supposons qu'une source produit des paires de photons EPR, qu'Alice a capturé un photon dans son laboratoire, et que Bob a capturé l' autre photon dans son laboratoire (figure 2). Quelle que soit la distance entre les deux laboratoires les photons (leur polarisation) restent intriqués dans l'état $|B_{00}\rangle$. Regardons le résultat de plusieurs mesures simples qu'Alice et Bob pourrait faire, chacun dans leur propre laboratoire. *Dans ce paragraphe nous supposons qu'ils ne peuvent pas communiquer entre eux les résultats de ces mesures* . Nous examinons trois situations précises où: Alice mesure avant / Bob mesure après; Bob mesure avant / Alice mesure après; Alice et Bob mesurent simultanément.

- *Alice mesure avant et Bob après.* L'appareil de mesure d'Alice est formé par les projecteurs $\{|\alpha\rangle\langle\alpha| \otimes I, |\alpha_\perp\rangle\langle\alpha_\perp| \otimes I\}$. Selon le postulat de la mesure,

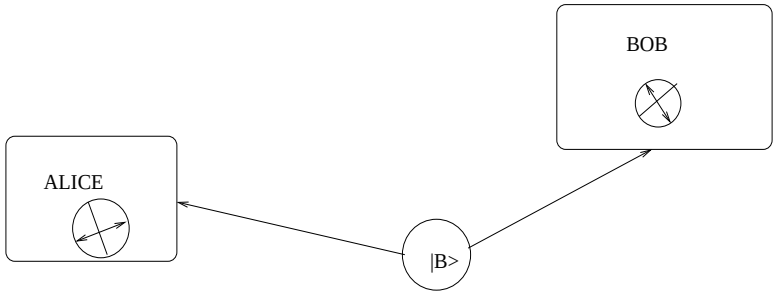


Figure 5.1 Alice et Bob partagent une paire intriquée.

l'état de Bell est projeté sur l'un des état

$$|\alpha\rangle\langle\alpha| \otimes I|B_{00}\rangle = \frac{1}{\sqrt{2}}|\alpha\alpha\rangle \rightarrow |\alpha\rangle \otimes |\alpha\rangle \qquad \text{avec prob } \frac{1}{2}$$

$$|\alpha_\perp\rangle\langle\alpha_\perp| \otimes I|B_{00}\rangle = \frac{1}{\sqrt{2}}|\alpha_\perp\alpha_\perp\rangle \rightarrow |\alpha_\perp\rangle \otimes \alpha_\perp\rangle \qquad \text{avec prob } \frac{1}{2}$$

Par conséquent Alice observe *son photon* dans létat $|\alpha\rangle$ ou $|\alpha_\perp\rangle$ avec probabilité 1/2 (Bob, de son coté, ne sait rien, et ne sait même pas qu'Alice a effectué une mesure!). Pour effectuer sa mesure Bob choisi une base $\{|\beta\rangle, |\beta_\perp\rangle\}$. Si son photon est dans l'état $|\alpha\rangle$ avant la mesure, celui-ci est projeté sur $|\beta\rangle$ avec probabilité $\cos^2(\alpha - \beta)$ ou $|\beta_\perp\rangle$ avec probabilité $\sin^2(\alpha - \beta)$. De même, si son photon est dans l'état $|\alpha_\perp\rangle$ il obtient le même résultat avec $\cos^2$ et $\sin^2$ interchangés. Le fait que Bob ne connait pas l'état initial de son photon, ou qu'il ne sait même pas si Alice a déja mesuré, ne devrait pas vous déranger : le point est qu'il fait une expérience spécifique (mesure dans la base $|\beta\rangle, |\beta_\perp\rangle$) et trouve un résultat net. Le résultat net dans le laboratoire de Bob est: le photon est dans l'état $|\beta\rangle$ avec probabilité $\frac{1}{2}$ ou $|\beta_\perp\rangle$ avec probabilité $\frac{1}{2}$.

- *Bob mesure d'abord et Alice après.* La même discussion montre que, si Bob effectue des mesures en premier (dans la base $|\beta\rangle, |\beta_\perp\rangle$), tandis que Alice dort, puis Alice mesure après (dans la base $|\alpha\rangle, |\alpha_\perp\rangle$). Le résultat net de chacune des parties est le même que précédemment.
- *Bob et Alice mesurent simultanément.* Vous pensez peut-être (?) que les résultats sont différents si les deux parties effectuent des mesures simultanées. Essayons. Supposons qu'Alice et Bob effectuent des mesures simultanées dans la base

$$\{|\alpha\beta\rangle; |\alpha\beta_\perp\rangle; |\alpha_\perp\beta\rangle; |\alpha_\perp\beta_\perp\rangle\}.$$

L'état de Bell

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|\gamma\gamma\rangle + |\gamma_\perp\gamma_\perp\rangle)$$

va être projeté sur l'un des quatre états de base. Donc, Alice sera en possession d'un photon dans l'état $|\alpha\rangle$ ou $|\alpha_\perp\rangle$ et Bob en possession d'un photon dans l'état $|\beta\rangle$ ou $|\beta_\perp\rangle$. La situation est exactement la même que précédemment! Il est très instructif de calculer les probabilités des états projetés respectifs. Alice constate que la probabilité de ses résultats $|\alpha\rangle$ (resp. $|\alpha_\perp\rangle$) valent

$$\frac{1}{2}\cos^2(\alpha\beta) + \frac{1}{2}\sin^2(\alpha\beta) = \frac{1}{2}$$

La même chose vaut pour Bob. Par conséquent, les conclusions qu'Alice et Bob déduisent de leurs mesures simultanées sont les mêmes que dans les cas non-simultanés ci-dessus. En fait l'ordre des mesures importe peu.

Résumons la situation. Lorsqu'Alice et/ou Bob effectuent des mesures locales successives ou simultanées sur leurs photons, quel que soit leur choix de base ils trouvent le photon dans l'un des deux états de la base choisie avec une probabilité $\frac{1}{2}$. En d'autres termes l'entropie de la distribution de probabilité de leurs résultats locaux est maximale (elle est égale à $\ln 2 = 1$ bit). Alice et Bob déduisent que leur photon est dans un état "maximalement désordonné". Ceci est remarquable. En fait, si ils ne savent pas que la source a produit une paire intriquée ou si personne ne leur dit que les deux photons sont intriqués, et qu'ils n'ont aucun moyen de communiquer leur mesures, ils n'ont aucun moyen de détecter l'intrication. Comme nous le verrons la situation est encore plus subtile. Alice et Bob peuvent affirmer que leurs photons sont intriqués si ils sont autorisés à communiquer. Par communiquer, nous entendons la transmission d'un message classique. Il semble que nous n'ayons aucun moyen de savoir si nous sommes intriqués avec des extraterrestres lointains dans l'Univers en faisant uniquement des expériences locales dans notre partie de l'univers. Pour le savoir il faut communiquer avec eux.

5.2 Inégalités de Bell

Nous avons vu que s'il n'y a pas de communication entre Alice et Bob, ils ne peuvent pas en déduire que les photons sont dans un état intriqué. Chacun de son coté peut seulement déduire des mesures locales que létat de son photon est hautement désordonné. Dans cette section, nous allons voir qu'en communiquant les résultats des mesures entre eux, Alice et Bob peuvent détecter l'intrication.

Les idées décrites ici ont été initiées par John Bell (1964), et motivée par un célèbre papier d'Einstein-Podolsky-Rosen (1935). Ces derniers affirmaient que les états intriqués ne constituent pas une "description complète" du système des deux particules, et pensaient qu'il devait exister une théorie de "type classique" qui donne la description complète du système. L'approche de Bell donne un critère expérimental pour décider si les corrélations d'une paire EPR *peut être décrite* ou *ne peut pas être décrite* par *une théorie classique* . L'idée générale

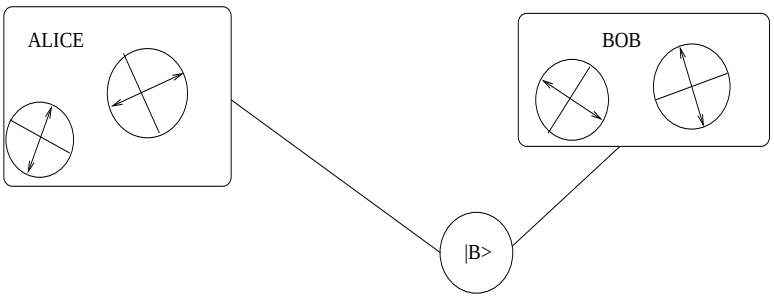


Figure 5.2 expérimental mis en place

est la suivante: si une paire de photons est décrite par une théorie classique alors certaines fonctions de corrélation appropriées des mesures d'Alice et Bob doivent satisfaire à des contraintes très particulières. Ces contraintes sont violées si la paire satisfait aux lois de la MQ. L'approche de Bell est capable de discriminer entre un vaste ensemble de théories classiques et la MQ. Les expériences fameuses d'Aspect-Grangier-Roger ont montré que la MQ gagne !

Le protocole expérimental. Une source S produit, à chaque instant n, une paire de photons. Un photon vole vers le laboratoire d'Alice et l'autre vers le laboratoire de Bob. Dans chaque laboratoire nos deux protagonistes fonctionnent de faàcon indépendante: les deux laboratoires sont distants, ne communiquent pas, et ne se soucient pas ce que l'autre fait.

- A chaque instant n, Alice utilise au hasard les analyseurs (Bob ne connait pas les choix d'Alice)

$$\{|\alpha\rangle,,|\alpha_\perp\rangle\} \qquad \text{ou} \qquad \{|\alpha'\rangle,|\alpha'_\perp\rangle\}$$

  pour mesurer la polarisation de son photon. Quand elle enregistre un clic dans le détecteur, elle définit $a_n = +1$ ou $a'_n = +1$. Lorsque le détecteur ne clique pas elle enregistre $a_n = -1$ ou $a'_n = -1$.
- A chaque instant n, Bob utilise au hasard les analyseurs (Alice ne connait pas les choix de Bob)

$$\{|\beta\rangle,|\beta_\perp\rangle\} \qquad \text{ou} \qquad \{|\beta'\rangle,|\beta'_\perp\rangle\}$$

  pour mesurer la polarisation de son photon. Quand il enregistre un clic dans le détecteur, il enregistre $b_n = +1$ ou $b'_n = 1$. Lorsque le détecteur ne clique pas il enregistre $b_n = -1$ ou $b'_n = -1$.
- une fois les mesures terminées Alice et Bob passent à une phase de communication classique. Par exemple, ils se rencontrent ou se téléphonent (ou bien tweetent des messages) et discutent de leurs mesures. Ils classent les résultats selon les quatre configurations expérimentales. A chaque instant temps n les arrangements possibles des analyseurs étaient

$$1 = (\alpha,\beta);\ 2 = (\alpha,\beta');\ 3 = (\alpha'\beta);\ 4 = (\alpha'\beta')$$

Pour chaque arrangement ils calculent les moyennes empiriques suivantes

$$\frac{1}{N_1}\sum_{n_1} a_{n_1} b_{n_1},\ \frac{1}{N_2}\sum_{n_2} a_{n_2} b'_{n_2},\ \frac{1}{n_3}\sum_{n_1} a'_{n_3} b_{n_3},\ \frac{1}{N_4}\sum_{n_4} a'_{n_4} b'_{n_4}$$

Ensuite, ils calculent la fonction de corrélation suivante

$$X_{exp} = \frac{1}{N_1}\sum_{n_1} a_{n_1} b_{n_1} + \frac{1}{N_2}\sum_{n_2} a_{n_2} b'_{n_2} - \frac{1}{n_3}\sum_{n_1} a'_{n_3} b_{n_3} + \frac{1}{N_4}\sum_{n_4} a'_{n_4} b'_{n_4}$$

Pour calculer cette corrélation Alice et Bob *doivent* communiquer pour échanger les variables a et b.

Prédiction des "théories classiques". Nous supposons que les quantités qu'Alice et Bob mesurent correspondent à observables A, A', B, B' qui prennent simultanément des valeurs précises a, a', b, b', indépendamment de la mesure. Fondamentalement, c'est comme dire qu'une particule a une certaine position et vitesse toutes deux bien d
'efinies (ici analogue à a *et* a') en toute ciconstance. C'est une hypothèse habituelle de la physique classique. En outre, nous supposons que les résultats d'Alice et Bob peuvent être modélisées par une distribution de probabilité jointe[2]

$$\mathrm{Prob}(a, a', b, b')$$

La prédiction théorique correspondant à *chaque* moyenne empirique ci-dessus est

$$\mathbf{E}[ab], \mathbf{E}[ab'], \mathbf{E}[a'b], \mathbf{E}(a'b')$$

La linéarité de l'espérance implique

$$\begin{aligned} X_{\text{theorique}} &= \mathbf{E}[ab] + \mathbf{E}[ab'] - \mathbf{E}[a'b] + \mathbf{E}(a'b') \\ &= \mathbf{E}[ab + ab' - a'b + a'b'] \end{aligned}$$

Remarquez maintenant que

$$ab + ab' - a'b + a'b' = a(b + b') + a'(b' - b)$$

et que

$$a(b + b') + a'(b' - b) = \pm 2$$

En effet, si $b = b'$, alors seul le premier terme survit et vaut ± 2, tandis que si $b \neq b'$ seulement le second terme survit et vaut aussi ± 2. La moyenne est forcément comprise dans l'intervalle $[-2, +2]$, et ainsi nous avons pour la prédiction des théories classiques

$$-2 \leq X_{\text{theorique}} \leq 2$$

[2] Cette seconde hypothèse sera justifiée ci-dessous. Elle suit d'une hypothèse de localité des résultats de mesure. Elle englobe un vaste ensemble de théories classiques possibles déterministes ou non.

C'est l'une des inégalités "de type Bell" obtenue par Clauser-Horne-Shimony-Holt (CHSH).

Afin d'obtenir ce résultat nous avons supposé l'existence d'une distribution conjointe $P(a, a', b, b')$ pour des valeurs des observables A, A', B et B' (c'est ce qui permet d'écrire $X_{\text{theorique}}$ comme la valeur moyenne d'une quantité comprise dans $[-2, +2]$). En fait, cette hypothèse n'est pas évidente a priori. Du point de vue expérimental, lorsque Alice et Bob se rencontrent, ils peuvent construire 4 histogrammes qui correspondent aux 4 arrangements possibles des analyseurs. ces quatres histogrammes correspondent à 4 distributions de probabilité:

$$P_1(a, b),\ P_2(a', b),\ P_3(a, b'),\ P_4(a', b')$$

Il n'est pas évident à priori que ces 4 distributions sont les marginales d'une distribution commume $P(a, a', b, b')$. Nous allons voir que pour une théorie classique locale cela doit effectivement être le cas.

Admettons que les lois de la physique sont "locales". Nous entendons par là que lorsque Alice (resp. Bob) effectuent ses mesures, les résultats d'Alice (resp. Bob) ne dépendent que de son propre choix local des analyseurs. C'est dire qu'étant donné un état du système décrit par un ensemble de variable classiques λ (appelées parfois variables cachées), les résultats des expériences d'Alice et Bob doivent être indépendantes. Elles sont modélisées par des distributions dépendant uniquement de la configuration locale des analyseurs et de l'état du système:

$$p_{\mathcal{A}}(a|\alpha, \lambda),\ p_{\mathcal{A}}(a'|\alpha'; \lambda),\ p_{\mathcal{B}}(b|\beta, \lambda),\ p_{\mathcal{B}}(b'|\beta'; \lambda)$$

Alors pour les choix α, $alpha'$, β, β' fixes les histogrammes d'Alice et Bob sont donnés par

$$P1(a, b) = \int d\lambda h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{B}}(b|\beta, \lambda)$$

$$P_2(a, b') = \int d\lambda h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{B}}(b'|\beta'; \lambda)$$

$$P_3(a', b) = \int d\lambda h(\lambda) p_{\mathcal{A}}(a'|\alpha'; \lambda) p_{\mathcal{B}}(b|\beta, \lambda)$$

$$P_4(a', b') = \int d\lambda h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{B}}(b|\beta, \lambda)$$

Ce sont les marginales d'une distribution de probabilité conjointe

$$P_{classe}(a, a', b, b') = \int d\lambda h(\lambda) p_{\mathcal{A}}(a|\alpha, \lambda) p_{\mathcal{A}}(a'|\alpha'; \lambda) p_{\mathcal{B}}(b|\beta, \lambda) p_{\mathcal{B}}(b'|\beta'; \lambda)$$

Remarquez que ce formalisme englobe les théories déterministes aussi. En effet les distribution ci-dessus, h, $p_{\mathcal{A}}$ et $p_{\mathcal{B}}$ pourraient être des distributions de Dirac.

Prédiction de la MQ pour un Etat Bell. Tout d'abord nous remarquons

que selon le formalisme quantique les mesures d' Alice et Bob sont des mesures des 4 observables (matrices hermitiennes)

$$A = (+1)|\alpha\rangle\langle\alpha| + (-1)|\alpha_\perp\rangle\langle\alpha_\perp| \qquad A' = (+1)\|\alpha'\rangle\langle\alpha'| + (-1)|\alpha'_\perp\rangle\langle\alpha'_\perp|$$

et

$$B = (+1)|\beta\rangle\langle\beta| + (-1)|\beta_\perp\rangle\langle\beta_\perp| \qquad B' = (+1)\|\beta'\rangle\langle\beta'| + (-1)|\beta'_\perp\rangle\langle\beta'_\perp|$$

A chaque instant n, l'état de la paire de photons est décrit par certains ket $|\Psi\rangle \in \mathbf{C}^2 \otimes \mathbf{C}^2$. La prédiction de la mécanique quantique pour les quatre moyennes empiriques de Alice et Bob est

$$\langle\Psi|A\otimes B|\Psi\rangle \ \langle\Psi|A\otimes B'|\Psi\rangle\langle\Psi|A'\otimes B|\Psi\rangle\langle\Psi|A'\otimes B'|\Psi\rangle$$

Pour la fonction de corrélation

$$X_{MQ} = \langle\Psi|A\otimes B|\Psi\rangle + \langle\Psi|A\otimes B'|\Psi\rangle - \langle\Psi|A'\otimes B|\Psi\rangle + \langle\Psi|A'\otimes B'|\Psi\rangle$$

Maintenant, nous calculons cette quantité pour l'état de Bell

$$|\Psi\rangle = |B_{00}\rangle$$

La première moyenne est calculée en exprimant l'état de Bell comme $\frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\alpha_\perp\alpha_\perp\rangle)$.

$$\begin{aligned}
\langle B_{00}|A\otimes B|B_{00}\rangle &= \frac{1}{2}\langle\alpha\alpha|A\otimes B|\alpha\alpha\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp|A\otimes B|\alpha_\perp\alpha_\perp\rangle \\
&\quad + \frac{1}{2}\langle\alpha\alpha|A\otimes B|\alpha_\perp\alpha_\perp\rangle + \frac{1}{2}\langle\alpha_\perp\alpha_\perp|A\otimes B|\alpha\alpha\rangle \\
&= \frac{1}{2}\langle\alpha|A|\alpha\rangle\langle\alpha|B|\alpha\rangle + \frac{1}{2}\langle\alpha_\perp|A|\alpha_\perp\rangle\langle\alpha_\perp|B|\alpha_\perp\rangle \\
&= \frac{1}{2}\cdot 1\cdot\Big(|\langle\alpha|\beta\rangle|^2 - |\langle\alpha|\beta_\perp\rangle|^2\Big) + \frac{1}{2}\cdot(-1)\cdot\Big(|\langle\alpha_\perp|\beta\rangle|^2 - |\langle\alpha_\perp|\beta_\perp\rangle|^2\Big) \\
&= \frac{1}{2}\Big(\cos^2(\alpha\beta) - \sin^2(\alpha-\beta)\Big) - \frac{1}{2}\Big(\sin^2(\alpha\beta) - \cos^2(\alpha-\beta)\Big) \\
&= \cos^2(\alpha\beta) - \sin^2(\alpha-\beta) = \cos 2(\alpha-\beta)
\end{aligned}$$

Effectuant des calculs similaires pour les autres moyennes, nous trouvons

$$X_{MQ} = \cos 2(\alpha-\beta) + \cos 2(\alpha-\beta') - \cos 2(\alpha'-\beta) + \cos 2(\alpha'-\beta')$$

Cette quantité est maximisée pour le choix suivant des angles (et toutes les rotations globales de ce choix, voir figure 4).

$$\alpha = 0,\ \alpha' = -\frac{\pi}{4},\ \beta = \frac{\pi}{8},\ \beta' = -\frac{\pi}{8}$$

et est égale à

$$X_{MQ} = \cos\frac{\pi}{4} + \cos\frac{\pi}{4} - \cos\frac{3\pi}{4} + \cos\frac{\pi}{4} = 2\sqrt{2}$$

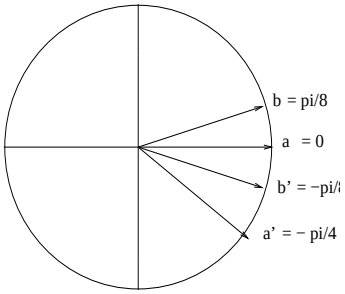


Figure 5.3 Choix optimal de l'orientation des l'analyseurs

Nous constatons que l'inégalité CHSH est violée car $2\sqrt{2} > 2$! Pour les trois autres états Bell on trouve le même résultat.

En fait la MQ prédit que les quatre histogrammes de Bob et Alice sont

$$P1(a,b) = \frac{1}{4}(1 + ab\cos 2(\alpha\beta))$$
$$P_2(a,b') = \frac{1}{4}(1 + ab'\cos 2(\alpha\beta'))$$
$$P_3(a',b) = \frac{1}{4}(1 + a'b\cos 2(\alpha'\beta))$$
$$P_4(a',b') = \frac{1}{4}(1 + a'b'\cos 2(\alpha'\beta'))$$

Par exemple: $P_2(+1,-1) = |\langle\alpha\beta'_\perp|B_{00}\rangle|^2 = \frac{1}{4}(1 - \cos 2(\alpha\beta))$. Il y a des choix particuliers des angles $\alpha, \beta, \alpha'\beta'$ pour lesquels ces histogrames *ne sont pas les marginales* d'une distribution commune $P(a,b,a',b')$. En effet si c'ètait le cas nous aurions du trouver $-2 \leq X \leq 2$. Ainsi les corrélations présentes dans les résultats de mesures ne peuvent pas être décrites par une distribution de probabilité classique. Elles sont décrite par l'état intriqué de Bell!

Remarque. On dit souvent que les états intriqués possèdent des "corrélation non-locales" car les deux photons peuvent être séparés d'une distance arbitraire, néanmoins l'inégalité de Bell est violée (c.a.d $X = 2\sqrt{2} > 2$). Néanmoins, toutes les intéractions connues sont locales au sens ou les forces décroissent avec la distance, et les mesures faites dans les laboratoires sont locales. Il faut donc faire attention lorsque l'on manipule les termes "local" et "non-local" en physique quantique. Les états intriqués posèdent des corrélations non-locales mais les interactions sont locales. De plus on ne peut pas mettre en évidence l'intrication en faisant uniquement de sopérations locales.

Expériences. Aspect-Grangier-Roger ont montré dans les années 1980 que l'expérience est en accord avec la MQ et non pas avec les théories classiques. Ces expériences nous forcent à abandonner la description classique. Une des difficultés expérimentales est de faire tourner les analyseurs d'Alice et Bob suffisamment

rapidement pour que les événements de mesure soient séparés par un intervalle de temps plus court que le temps que mettrait la lumière pour parcourir la distance séparant Alice et Bob. Sinon, on pourrait argumenter qu'une certaine forme de communication classique ou interaction conspire pour établir les corrélations non-locales pendant la mesure.

5.3 La téléportation quantique

Supposons qu'Alice et Bob soient séparés dans l'espace et que Alice possède un qubit dans l'état

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

L'état (c.a.d α et β) n'est pas nécessairement connu pour Alice et n'est pas connu pour Bob. Ils partagent également une paire intriquée

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

et ont aussi à leur disposition un canal de communication classique.

Nous allons expliquer que par l'envoi de seulement deux bits classiques d'information sur le canal classique, Alice peut *téléporter* l' état de son qubit vers Bob. Ici, *téléportation* signifie que $|\Phi\rangle$ est détruit dans le laboratoire d'Alice et est reconstruit dans le laboratoire de Bob. Notez que la destruction de $|\Phi\rangle$ dans le laboratoire d'Alice est nécessaire à cause du théorème de non-clonage. Après le processus de téléportation, Bob sait qu'il possède l' état $|\Phi\rangle$, mais ne connait toujours pas l'état lui-même (c'est à dire qu'il ne connait pas α et β). Nous soulignons que le processus de téléportation nécessite un transport physique d'information classique (stockée dans de la matière) dans la phase de communication classique entre Alice et Bob. Bien entendu, cette phase de communication classique ne peut pas se produire à une vitesse supérieure à celle de la lumière, de sorte que l'ensemble du processus de téléportation ne viole pas les principes de la relativité. Nous notons également que le support matériel de l'état $|\Phi\rangle$ (par exemple, la polarisation du photon, le spin de l'électron, les degrés de liberté atomiques ou moléculaires) n'est pas nécessairement le même dans les laboratoires d'Alice et de Bob .

On résume parfois la téléportation par la " loi“ suivante

$$\text{teleporter}, 1\,\text{Qbit}, =, \text{communiquer}, 2, \text{Cbits}, +, \text{partager1}, \text{paire}, \text{EPR}$$

La téléporation peut être considérée comme une forme de communication entre Alice et Bob qui partagent une canal classique et un "canal constitué de paires intriquées" (canal EPR).

Le protocole.

- Une source produit une paire EPR de particules dans l'état de Bell $|B_{00}\rangle_{23}$.

La particule, appelée particule 2 est envoyée à Alice et la particule, appelée particule 3 est envoyée á Bob. L' espace de Hilbert du système intriqué 23 est $\mathcal{H}_2 \otimes \mathcal{H}_3 = C^2 \otimes C^2$.

- Alice prépare une particule, appelée 1, dans l'état $|\Phi\rangle_1 = \alpha|0\rangle + \beta|1\rangle$. L'espace de Hilbert de la particule 1 est $\mathcal{H}_1 = C^2$.
- L' espace total de Hilbert du système composite 123 est $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 = C^2 \otimes C^2 \otimes C^2$. L'état complet du système est

$$|\Psi\rangle = |\Phi\rangle_1 \otimes |B_{00}\rangle_{23}$$

A ce stade, un bref calcul facilitera la discussion qui suit

$$|\Psi\rangle = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

- Alice fait une mesure locale dans son laboratoire, á savoir sur les particules 12. Elle utilise un appareil modélisé par la base de mesure dans $\mathcal{H}_1 \otimes \mathcal{H}_2$

$$\{|B_{00}\rangle_{12}, |B_{01}\rangle_{12}, |B_{10}\rangle_{12}, |B_{11}\rangle_{12}\}$$

Les projecteurs associés pour l'ensemble du système sont

$$P_{00} = |B_{00}\rangle\langle B_{00}|\otimes I_3, P_{01} = |B_{01}\rangle\langle B_{01}|\otimes I_3, P_{10} = |B_{10}\rangle\langle B_{10}|\otimes I_3, P_{11} = |B_{11}\rangle\langle B_{11}|\otimes I_3$$

Comme d'habitude, le résultat de la mesure est l'un des quatre états projetés possibles (à une normalisation près; vérifier ce calcul et aussi que la probabilité de chaque résultat est $\frac{1}{4}$)

$$P_{00}|\Psi\rangle = \frac{1}{2}|B_{00}\rangle_{12} \otimes (\alpha|0\rangle_3 + \beta|1\rangle_3)$$

$$P_{01}|\Psi\rangle = \frac{1}{2}|B_{01}\rangle_{12} \otimes (\beta|0\rangle_3 + \alpha|1\rangle_3)$$

$$P_{10}|\Psi\rangle = \frac{1}{2}|B_{10}\rangle_{12} \otimes (\alpha|0\rangle_3 - \beta|1\rangle_3)$$

$$P_{11}|\Psi\rangle = \frac{1}{2}|B_{11}\rangle_{12} \otimes (-\beta|0\rangle_3 - \alpha|1\rangle_3)$$

- Pour chacun de ces résultats possibles, Bob possède l'un des quatre états

$$\begin{aligned}
\alpha|0\rangle_3 + \beta|1\rangle_3 &= |\Phi\rangle \\
\beta|0\rangle_3 + \alpha|1\rangle_3 &= X|\Phi\rangle \\
\alpha|0\rangle_3 - \beta|1\rangle_3 &= Z|\Phi\rangle \\
\beta|0\rangle_3 - \alpha|1\rangle_3 &= iY|\Phi\rangle
\end{aligned}$$

mais il ne sait pas lequel, étant donné qu'il ne connait pas le résultat de la mesure d'Alice.

- Alice connait le résultat de sa mesure (dans son laboratoire). C'est l'un des quatres états de Bell. Ce résultat peut être codé par deux bits classiques, puis communique à Bob sur le canal classique,

$$00, 01, 10, 11$$

Dès que Bob reçoit le message d'Alice, il sait qu'elle a terminé ses opérations et possède deux bits d'information nécessaires pour décider quelle est l'opération *unitaire* qu'il doit effectuer sur son état afin de récupérer $|\Phi\rangle$,

$$\begin{aligned} I(\alpha|0\rangle_3 + \beta|1\rangle_3) &= |\Phi\rangle \\ X(\beta|0\rangle_3 + \alpha|1\rangle_3) &= |\Phi\rangle \\ Z(\alpha|0\rangle_3 - \beta|1\rangle_3) &= |\Phi\rangle \\ -iY(\beta|0\rangle_3 - \alpha|1\rangle_3) &= |\Phi\rangle \end{aligned}$$

5.4 Codage superdense

Supposons qu'Alice et Bob ont mis en place un canal quantique sur lequel ils peuvent envoyer qubits (par exemple une fibre optique sur laquelle les photons voyagent). On suppose aussi qu'Alice et Bob partagent une paire EPR. Combien de bits d'information classiques peuvent-ils communiquer en envoyant un seul qubit à travers le canal quantique?

La réponse: 2 bits d'information classique peuvent être transmis par Alice à Bob, en envoyant seulement 1 Qbit tant qu'ils partagent une paire EPR. Le protocole qui réalise ceci s'appelle "codage superdense" (dense coding).

La "loi" du codage superdense peut être résumée ainsi:

$$\text{communiquer}, 2, \text{Cbits}, = \text{envoiyer}, 1, \text{Qbit} + \text{partager}, 1, \text{paire}, \text{EPR}$$

Le protocole.

- Une paire EPR dans l'état $|B_{00}\rangle$ est préparée par une source. Chaque particule de la paire est envoyée à Alice et Bob .
- Alice veut communiquer deux bits d'information à Bob :
  - Pour envoyer 00 elle laisse sa particule intacte (ou applique la matrice unitaire I) et envoie sa particule à Bob. Bob reàcoit la particule et est maintenant en possession de l'état $|B_{00}\rangle$ tout entier

$$|B_{00}\rangle$$

  - Pour envoyer 01 elle applique la matrice unitaire X à sa particule, puis envoie sa particule à Bob. Bob est maintenant en possession de la paire dans l'état

$$X_1 \otimes I_2|B_{00}\rangle = |B_{01}\rangle$$

- Pour envoyer 10, elle applique la matrice unitaire Z à sa particule, puis envoie sa particule. Bob est maintenant en possession de la paire dans l'état

$$Z_1 \otimes I_2 |B_{00}\rangle = |B_{10}\rangle$$

- Pour envoyer 11, elle applique la matrice unitaire iY à sa particule, puis envoie physiquement sa particule. Bob est maintenant en possession de la paire dans l'état

$$(IY)_1 \otimes I_2 |B_{00}\rangle = |B_{11}\rangle$$

- Bob a maintenant la paire EPR 12 dans un état $|B_{xy}\rangle$. Afin de déterminer les deux bits d'information classique qu'Alice a envoyé il doit décider quel est l'état de Bell dont il dispose. Comme Bob sait qu'il possède l'un des quatre états de Bell dans son laboratoire, il peut faire une mesure locale dans la base de Bell, et accéder aux informations xy .

Expériences. La téléportation et le codage superdense ont été réalisés expérimentalement. Un résumé du sujet peut être trouvé dans "Les dossiers de la Recherche" no 18, Février 2005 "L ' étrange Pouvoir de l' intrication quantique", par N. Gisin .

6 Modèle des Circuits et Algorithmes Quantique

Ce chapitre est une première introduction au calcul quantique. Après une brève introduction historique et une discussion de la notion de circuit classique, nous introduisons le modèle de Deutsch des "circuits quantiques" (1995). Comme nous allons le voir ce modèle sert à définir ce qui sera pour nous un algorithme quantique, tout en fournissant une représentation très concrète de ces algorithmes. Enfin, nous illustrons ces notions grâce à un algorithme quantique simple mais important, l'algorithme de Deutsch et Josza. Cet algorithme quantique contient déjà la plupart des ingrédients d'une classe plus large, qui traite le problème plus général de la recherche de symétries cachées. Le célèbre algorithme de Shor (1997), permettant la factorisation d'un nombre entier en temps polynomial (par rapport aux nombres de bits de l'entier) appartient à cette classe. Celui-ci fera l'objet des chapitres suivants. Il est suspecté, mais pas démontré, que cette famille d'algorithmes quantiques permet une accélération exponentielle du temps de calcul, par rapport aux algorithmes classiques.

6.1 Brève introduction historique

Un calcul est de facon ultime réalisé par un dispositif physique. Il est donc naturel de se demander quelles sont les limites fondamentales que les lois de la physique imposent au calcul. Un travail précurseur fut celui de Landauer (dans les années 60-70) qui montra que l'effacement d'un bit - un processus irréversible - est toujours accompagné d'une dissipation de chaleur. Essentiellement, ceci provient de l'augmentation de l'entropie du système due a l'effacement du bit (perte d'information) et des lois de la thermodynamique reliant la variation d'entropie d'un système au flux de chaleur entre le système et son environnement. En conséquence, tout calcul utilisant des portes logiques *irréversibles* (par exemple AND, OR) dissipe de la chaleur. Mais existe-il un principe fondamental qui nécessite absolument une dissipation minimale de chaleur lors d'un calcul ? Ou bien pourrait-on, en théorie du moins, éliminer la dissipation de chaleur lors du calcul ? Une *réponse positive* à cette deuxième question a été présentée par Bennett, Benioff et d'autres. Plus précisément, *tout calcul irréversible peut être rendu réversible*, grâce à des portes élémentaires appropriées. Néanmoins il y a un cout: l'espace de stockage doit être augmenté pour éliminer les effacements.

En l'absence de la chaleur générée par un calcul réversible, lorsque le support physique des bits atteint les dimensions moléculaires ou atomiques et que la température du système est maintenue très basse, le comportement quantique de la matière et la cohérence des états quantiques (le principe de superposition) deviennent importants. Il est naturel de se poser la question suivante: quels sont les effets du comportement quantique de la matière sur le calcul ? Est ce que les effets quantiques aident, ou bien au contraire apportent-ils de nouvelles limites ?

Ces questions ont été soulevées et discutées par Feynman, Benioff et Manin au début des années 1980. En principe la MQ n'apporte pas de nouvelles limitations. Au contraire ! Le principe de superposition appliqué à des systèmes à plusieures particules (plusieurs qubits) nous permet d'effectuer des "calculs parallèles". Ce "paralélisme quantique" accélère les calculs classiques, et parfois même de facon exponentielle. Cela a été reconnu notamment par Feynman qui a fait valoir que les ordinateurs classiques ne peuvent simuler des processus quantiques "efficacement" (du point de vue du temps de calcul). Feynman a suggérer que nous devrions construire des "machines quantiques" pour simuler efficacement les processus quantiques.

La raison fondamentale pour laquelle le calcul classique ne peut pas simuler efficacement les processus quantiques est la suivante. Un état général quantique de n bits quantiques contient une superposition de 2^n "états classiques":

$$|\Psi\rangle = \sum_{b_1 \dots b_N \in \{\{0,1\}\}^N} C(b_1, \dots, b_N)|b_1, \dots, b_N\rangle$$

Ici $|b_1, \dots, b_N\rangle = |b_1\rangle \otimes \dots \otimes |b_N\rangle$ (avec $b_i = 0, 1$) sont les états de la base dite "computationnelle". Une simulation classique de l'évolution du ket $|\Psi\rangle$ doit effectuer essentiellement 2^n calculs pour l'évolution de suite binaire classique $(b_1 \dots b_N)$. Au contraire, la dynamique quantique unitaire U agit sur $|\Psi\rangle$ dans son ensemble (ou en parallèle sur chaque ket $|b_1 \dots b_N\rangle$). Un dispositif physique réalisant la dynamique unitaire U sur $|\Psi\rangle$ peut être considéré comme un ordinateur quantique.

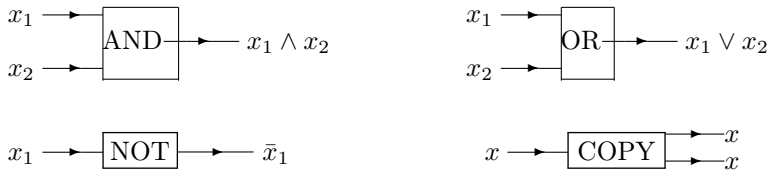
Un calcul classique peut être représenté par un modèle de circuit construit à partir d'un ensemble donné de portes élémentaires universelles agissant de manière récursive sur l'entrée du calcul. En 1985 David Deutsch a montré que la même chose est valable dans le cas quantique. Notamment, toute évolution unitaire peut être assez bien approchée par un ensemble universel de portes quantiques universelles.

Il existe aussi d'autres modèles d'ordinateur quantique mais le modèle de Deutsch - un modèle de circuit quantique - est le plus populaire aujourd'hui. Un des buts de ce chapitre est d'expliquer ce modèle. Une des raisons de sa popularité est qu'il s'agit d'un modèle universel: en principe, tout calcul quantique peut être représenté comme un circuit quantique construit à partir d'un ensemble restreint de porte logiques quantiques. De plus cette représentation est relativement concrète.

Il existe aussi une notion de machine de Turing quantique (analogue aux machines de Turing classiques) qui est le cadre naturel pour discuter des classes de complexité quantiques. Il a été démontré que le modèle de machine de Turing quantique est équivalent au modèle des circuits quantiques. Cet aspect ne sera pas abordé ici.

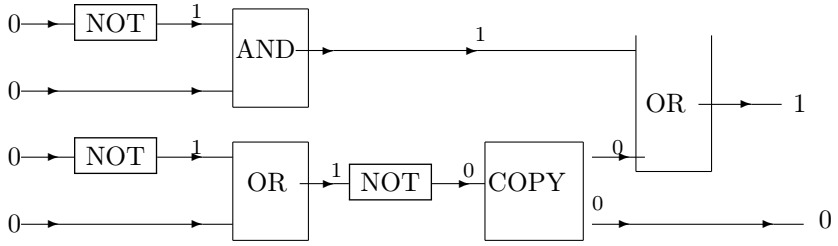
6.2 Modèle des circuits pour le calcul classique

Nous discutons brièvement le calcul classique basé sur les circuits booléens. Considérons les portes logiques classiques de base $x_i \in \mathbf{F}_2 = \{0, 1\}$.



L'opération COPY s'appelle aussi parfois FANOUT. Cet ensemble de portes peut être utilisé pour définir les circuits Booléens.

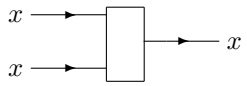
Un circuit Booléen est un graphe acyclique (sans cycles) dirigé (les liens ont une direction) avec n bits d'entrée et m bits de sortie. L'entrée peut toujours être initialisée à $(0 \ldots 0)$ car tout $(x_1 \ldots x_n)$ est obtenu par une série de portes NOT. La figure suivante illustre cette definition.



Un celèbre théorème d'Emil Post (∼1950) montre que toute fonction $f : \mathbf{F}_2^n \to \mathbf{F}_2^m$ peut être réalisée par un circuit Booléen. Plus précisément, pour toute fonction $f : \mathbf{F}_2^n \to \mathbf{F}_2^m$ il existe un circuit Booléen qui applique les entrées $(x_1 \ldots x_n)$ sur les sorties $(y_1 \ldots y_m) = f(x_1 \ldots x_n)$. Le circuit est entièrement construit avec les portes NOT, AND, OR, COPY et est un graphe acyclique dirigé. On dit que l'ensemble des portes (NOT, AND, OR, COPY) est universel.

La porte NOT est logiquement réversible. Cela veut dire qu'à partir de la sortie il est possible de récupérer l'entrée. Les portes AND et OR elles, sont logiquement irréversibles. Il est impossible de reconstruire l'entrée à partir de la

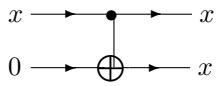
sortie. L'irréversibilité logique entraine l'irréversibilité physique c.a.d une dissipation de chaleur lors du calcul. En effet la perte d'information et l'augmentation d'entropie est reliée à un flux de chaleur du système vers l'environnment. La porte COPY quand à elle, est logiquement réversible, mais physiquement irréversible. En effet l'operation inverse



efface un bit et, comme Landauer l'a montré, cela entraîne une dissipation de chaleur.

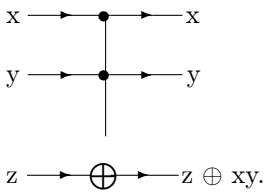
Bennett a montré que n'importe quel circuit Booléen peut être simulé ou remplacé par un circuit réversible. De plus il existe un ensemble universel de portes logiques réversibles (logiquement et physiquement réversibles). Nous n'allons pas donner cette preuve ici mais nous contenter de l'idée essentielle: on peut toujours remplacer les portes AND, OR et COPY par des portes réversibles à condition d'utiliser des bits auxiliaires.

Commencons par la porte COPY. Elle peut être remplacée par



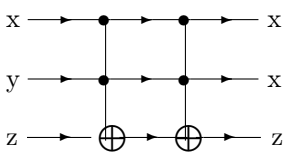
qui est une porte control-NOT (aussi notée CNOT) réversible utilisant deux bits. Le bit de stockage est égal à 0 dans l'entrée.

Pour les portes AND et OR nous utilsons la porte de Toffoli. Celle-ci n'est rien d'autre qu'un CCNOT (control-control-NOT) et utilise trois bits.



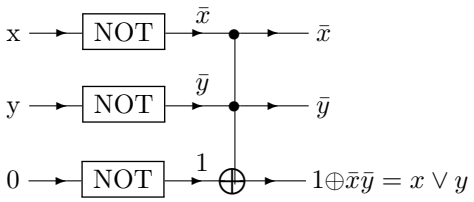
ou $\mathrm{T}(x, y, z) = (x, y, z \oplus xy)$.

Cette porte flip le bit z si les deux bits de controle x et y sont égaux à 1. Sinon z est inchangé. La porte de Toffoli est réversible car



or $\mathrm{T}^2(\mathrm{x}, \mathrm{y}, \mathrm{z}) = (\mathrm{x}, \mathrm{y}, \mathrm{z})$

Si $z = 0$, $T(x, y, 0) = (x, y, xy)$ retourne $x \wedge y$ pour le troisième bit. Pour la porte OR on utilise



Résumons: un circuit Booléen utilisant {AND, OR, COPY, NOT} peut être remplacé par un circuit utilisant les portes universelles {CNOT; Toffoli; NOT}. L'ensemble {AND, OR, COPY, NOT} contient uniquement des portes à un et deux bits, alors que {CNOT; Toffoli; NOT} fait intervenir une porte à trois bits (Toffoli). On peut montrer qu'il n'est pas possible de se passer de portes à tris bits si on veut la réversibilité d'un circuit classique. Nous verrons que dans le cas quantique cela est possible !

6.3 Circuits quantiques.

Les circuits quantiques sont analogues aux circuits classiques. En particulier, ils sont construits à partir d'un petit ensemble de "portes quantique" élémentaires. Une "porte quantique" n'est rien d'autre qu'une opération unitaire qui agit sur un petit nombre de qubits (typiquement un ou deux qubits). Ces portes sont réversibles car une opération unitaire est inversible, en effet $UU^\dagger = U^\dagger U = I$. Nous verrons dans des chapitres ultérieurs comment elles sont réalisées en pratique. Nous commencons par discuter certaines de ces portes élémentaires.

*

Portes à un qubit

Les portes à un qubit sont des matrices unitaires qui agissent sur les vecteurs d'état de l'espace d'Hilbert $\mathbf{C}^2$. Certaines de ces matrices joueront un role particulièrement important.

- Les trois "matrices de Pauli" $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $iY = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Ce sont bien des matrices unitaires (attention: Y n'est pas unitaire mais hermitienne, néanmoins iY est unitaire; X et Z sont unitaires et hermitiennes).

$$|b\rangle \longrightarrow \boxed{\text{X}} \longrightarrow |\bar{b}\rangle$$

$$|b\rangle \longrightarrow \boxed{\text{iY}} \longrightarrow (-1)^{b+1}|\bar{b}\rangle$$

$$|b\rangle \longrightarrow \boxed{\text{Z}} \longrightarrow (-1)^{b}|b\rangle$$

La porte X n'est rien d'autre que la porte NOT quantique. Dans le cas quantique l'entrée peut être une superposition cohérente des états $\{|0\rangle, |1\rangle\}$. Par exemple

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

Ainsi l'action de la porte NOT est beaucoup plus générale dans le cas quantique. Cette remarque est simple mais cruciale et profonde (et s'applique à toutes les portes quantiques discutées ci-dessous) !

- La porte de Hadamard $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$|b\rangle \longrightarrow \boxed{\text{H}} \longrightarrow H|b\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$

Cette porte n'a pas d'analogue classique.

- La porte $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

$$|b\rangle \longrightarrow \boxed{\text{T}} \longrightarrow e^{ib\pi/4}|b\rangle = \begin{cases} |0\rangle \\ e^{i\pi/4}|1\rangle \end{cases}$$

Elle agit sur les superpositions comme

$$T(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta e^{i\pi/4}|1\rangle$$

- La porte $S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

$$|b\rangle \longrightarrow \boxed{\text{S}} \longrightarrow e^{ib\pi/2}|b\rangle = \begin{cases} |0\rangle \\ i|1\rangle \end{cases}$$

Elle agit sur les superpositions comme

$$S(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + i|1\rangle$$

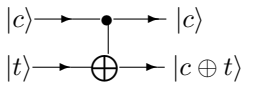
On peut montrer que toute matrice unitaire 2×2 peut être approximée avec une précision arbitraire par des produits des matrices élémentaires H et T. Notez que $S = T^2$.

*

Portes à deux qubits

Les portes à deux qubits sont des matrices unitaires qui agissent sur les vecteurs d'état de l'espace d'Hilbert $\mathbf{C}^2 \otimes \mathbf{C}^2$. La plus importante est la porte control-NOT quantique.

- La porte CNOT (controlled not) est définie par:



Dans la base

$$|0\rangle \otimes |0\rangle \; ; \quad |0\rangle \otimes |1\rangle \; ; \quad |1\rangle \otimes |0\rangle \; ; \quad |1\rangle \otimes |1\rangle$$

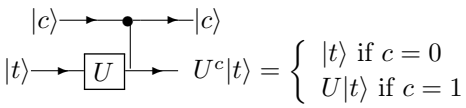
$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

la représentation matricielle est

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

Nous remarquons que cette porte agit en général sur des superpositions cohérentes d'états à deux qubits.

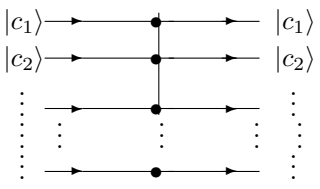
- Une généralisation importante est la porte control-U ou U est une opération unitaire à un qubit:

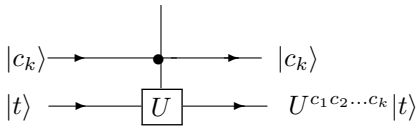


*

Portes muti-control-U

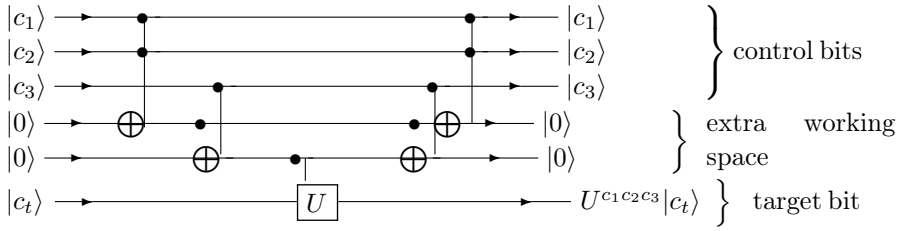
Une généralisation des portes précédentes est



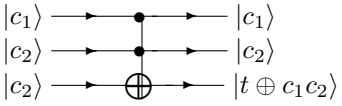


La porte U agit sur le dernier bit si tous les bits de controle sont égaux à 1. A nouveau il est important de remarquer que ces portes agissent sur des superpositions cohérentes d'états de base de l'espace de Hilbert $\mathbf{C}^2 \otimes \ldots \mathbf{C}^2$. Ce sont des matrices $2^n \times 2^n$.

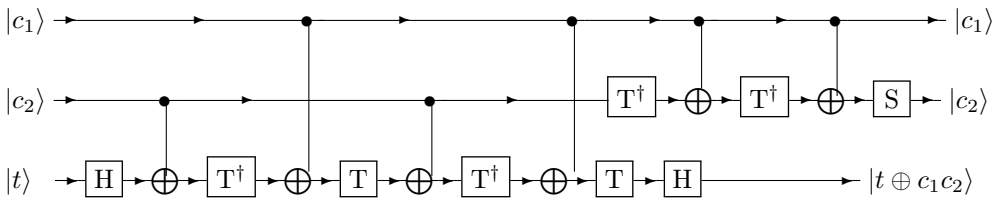
En augmentant le nombre de qubits auxiliaires la porte multi-control-U peut être réalisée grâce à une concaténation d'un control-control-NOT and un control-U. En effet (exercices):



La porte control-control-NOT gate s'appelle aussi porte de Toffoli quantique (la différence avec la porte classique est que les entrées peuvent être des superpositions d'états). Remarquablement cette porte quantique peut être représentée par des portes à un & deux qubits {T, S, H, CNOT}. On vérifie que:



est équivalent au circuit suivant (exercices):



Résumons cette discussion: Toute porte multi-control-U de dimension $2^n \times 2^n$ peut être réalisée grace à l'ensemble {T, S, H, CNOT, U} où U est une porte à un qubit. De plus nous avons aussi vu que U peut être approximée avec une précision arbitraire par un produit de matrices H et T.

*

Le modèle des circuits quantiques de Deutsch

Le dernier résultat du paragraphe précédent peut être généralisé. Un théorème important affirme que toute opération unitaire agissant sur l'espace à n qubits (c.a.d toute matrice $2^n \times 2^n$) peut être approximée avec une précision arbitraire par l'ensemble des portes {T, S, H, CNOT}. Ce théorème est à la base du modèle des circuits quantiques.

La complexité du circuit dépendra du nombre de matrices utilisées pour approximer l'opération unitaire à n qubits. Nous verrons par exemple que l'opération unitaire utilisée pour la factorisation des entiers requiert $O(\text{poly}N)$ portes quantiques élémentaires. Cela n'est pas possible avec un circuit classique. Néanmoins on sait qu'il existe des matrices unitaires qui requièrent un nombre exponentiellement grand (en n) de portes élémentaires.

Définissons maintenent le modèle des circuits:

a) Un circuit quantique est graphe dirigé acyclique avec les vertex qui sont les portes {T, S, H, CNOT}. Les liens "portent" des qubits ($\alpha|0\rangle + \beta|1\rangle$).
b) L'entrée est donnée par l'état produit:

$$|0\rangle \otimes ... \otimes |0\rangle$$

c) La sortie est le résultat de l'évolution unitaire. Cette sortie prend la forme générale:

$$|\Psi\rangle = \sum_{c_1 \ldots c_n} A(c_1 ... c_n)|c_1 c_2 ... c_n\rangle$$

ou $A(c_1 ... c_n)$ sont des coefficients complexes et $|c_1 c_2 ... c_n\rangle = |c_1\rangle \otimes \ldots |c_n\rangle$ sont les états de la base computationnelle.
d) Finalement une opération de mesure est effectuée sur $|\Psi\rangle$ avec un appareil mesurant dans la "base computationnelle" $\{|c_1 c_2 ... c_n\rangle, c_i = 0, 1\}$. Le résultat de l'opération de mesure est l'état $|c_1 ... c_n\rangle$ avec probabilité $|\mathrm{A}(c_1 ... c_n)|^2$ (règle de Born). Le résultat du calcul quantique est donc un résultat probabiliste. En pratique l'algorithme est bon si la probabilité est concentrée sur le résultat cherché. La plupart du temps on répète l'expérience (le calcul du circuit) pour amplifier cette probabilité (nous verrons cela en pratique).

Remarquons les points importants:

1 Des "qutrits" au lieu des "qubits" ne changeraient rien de fondamental (et la nature offre des qubits).
2 Faire les opérations de mesure à des stades intermédiares ou bien à la fin ne change rien.
3 Faire les opérations de mesure dans une autre base est équivalent à faire des opération de changement de base - qui sont unitaires car toutes les bases de mesure sont orthonormées - et donc à changer le circuit et faire la mesure

dans la base computionnelle. Néanmoins cela peut modifier la complexité (la réduire ou l'agrandir).

4 Commencer avec une autre entrée est aussi équivalent à ajouter des opérations unitaires et donc à changer le circuit et initialiser avec l'entrée $|0, \cdots, 0\rangle$. Néanmoins cela peut modifier la complexité (la réduire ou l'agrandir)..

5 Il existe aussi d'autres ensembles de portes universelles.

6 Le calcul quantique est réversible (pas de perte d'information, pas d'augmentation d'entropie et pas de dissipation de chaleur) car le circuit est une opération unitaire, tant que l'opération de mesure n'a pas été effectuée.

7 Une opération classique réversible peut être représentée par une opération unitaire quantique. En effet:

$$\tilde{f}(x_1...x_n, y) = (x_1...x_n, y \oplus f(x_1...x_n))$$

induit l'unitaire

$$U_f|x_1...x_n, y\rangle = |x_1...x_n, y \oplus f(x_1...x_n)\rangle.$$

Si la sortie $f(x_1...x_n)$ possède m composantes on prend y avec m composantes et l'addition modulo 2 (le XOR) est faite composante par composante. On vérifie aisément que U_f est unitaire, en vérifiant que la matrice préserve le produit scalaire.

8 Le point précédent montre que tout calcul réversible classique est contenu dans le modèle des circuits quantiques.

9 La puissance du calcul quantique vient de l'action simultané ou parallèle de l'évolution unitaire sur toutes les "suites classiques" $c_1 \dots c_n$ d'un état de n qubits. C'est ce qu'on appelle parfois le parallélisme quantique: celui-ci provient des principes 1 (superposition) et 5 (produit tensoriel des systèmes composés) mis ensemble. La complexité du calcul est donné par la taille du circuit. Le résultat est aléatoire. En général il faut répéter un certain nombre de fois que le calcul quantique pour obtenir le résultat voulu avec une probabilité proche de 1. Cette répétition peut augmenter la complexité.

6.4 Le problème de Deutsch-Jozsa

L'algorithme de Deutsch et Jozsa est probablement l'algorithme quantique le plus simple. Dans sa version initiale il fut inventé par David Deutsch dans son article fondateur[1] en 1985. L'algorithme fut ensuite amélioré par Deutsch et Jozsa (1992) et finalement par Cleve-Ekert-Macchiavello-Mosca (1998). Cette version finale fait clairement apparaître que l'algorithme est le prototype d'une classe plus vaste, étudiée dans les chapitre ultérieurs, basée sur la *transformée de Fourier quantique* et le *principe d'interférence des chemins quantiques*. De

[1] *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer* Proc. Roy. Soc of London A **400** pp 97-117 (1985)

Figure 6.1 Oracle classique retournant les valeurs de la fonction f.

plus, il constitue une très bonne illustration d'un cas où l'on peut tirer parti du *parallélisme quantique* de facon assez spectaculaire.

Formulons d'abord le problème à résoudre. Soit

$$f : \mathbf{F}_2^n \to \mathbf{F}_2, \qquad (x_1 \dots x_n) \mapsto f(x_1 \dots x_n) \in \{0, 1\}$$

une fonction booléenne dont on sait a priori qu'elle est *constante* ou *balancée*. La fonction est constante si l'image prend toujours la même valeur quelle que soit l'arguement $(x_1 \dots x_n)$. Notez qu'il y a 2^n arguments possibles. *Balancée* signifie que pour une moitié des arguments (c.a.d 2^{n-1}) elle prend la valeur 0 et pour l'autre moitié (c.a.d 2^{n-1}) elle prend la valeur 1.

Le problème de Deutsch-Jozsa est un *problème de décision avec Oracle*. Cela veut dire que l'on ne connaît pas la fonction f mais que l'on a à disposition un *Oracle* qui donne la réponse $f(x_1 \dots x_n)$ pour toute entrée $x_1 \dots x_n$ qui lui est soumise. Le problème est de décider si f est constante. Le nombre de questions nécessaires à l'Oracle détermine la complexité temporelle de la résolution. Le but est de prendre la décision correcte en posant le moins de questions possibles.

Discutons d'abord la solution classique. Si on se limite à utiliser un *algorithme déterministe*, il existe des fonctions f pour lesquelles la complexité temporelle est de $2^{n-1}+1$, c'est-à-dire exponentielle par rapport à la taille des entrées. En effet supposons que f soit constante et prenne la valeur 0 si bien que l'Oracle retourne toujours la réponse 0. Si l'on pose strictement moins de $2^{n-1}+1$ questions à l'Oracle on n'a aucun moyen de savoir si la prochaine réponse sera aussi 0. Par contre si à la $2^{n-1}+1$ ième question la réponse est 0 alors on peut affirmer avec certitude que la fonction n'est pas balancée car si elle l'était cette réponse aurait été 1.

Notons que si la fonction est balancée le nombre minimum de questions à poser est deux et le maximum est $2^{n-1}+1$. Le point important est qu'il existe des situations défavorables qui nécessitent un nombre exponentiel de questions.

Nous allons voir qu'il existe un algorithme quantique qui permet de déterminer si f est balancée ou constante avec une et une seule utilisation de l'Oracle et ceci quel que soit la fonction f. Cela est assez spectaculaire. Notons que par rapport à un algorithme classique déterministe, le gain est exponentiel.

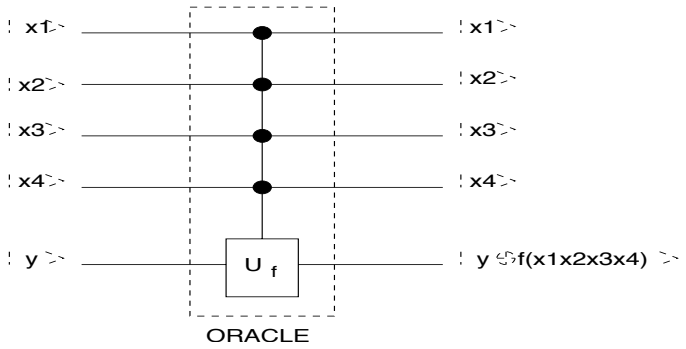


Figure 6.2 L'Oracle quantique retourne le résultat de f stocké dans les bits auxiliaires

6.5 L'Oracle quantique

Pour chaque n on construit un circuit qui constitue l'algorithme. Les constituants du circuit sont la porte quantique de Hadamard et un *Oracle quantique*. Ici nous discutons la modélisation de l'Oracle.

L'Oracle quantique est une porte donnée (par la Nature par exemple; c'est-à-dire que cela pourrait être un système physique) qui effectue l'opération *unitaire* suivante :

$$U_f|x_1 \dots x_m, y\rangle = |x_1 \dots x_m, y \oplus f(x_1 \dots x_m)\rangle$$

Cet opérateur agit sur un Ket de Dirac à plusieurs qubits appartenant à l'espace

$$\underbrace{\mathbf{C}^2 \otimes \mathbf{C}^2 \dots \mathbf{C}^2}_{n \text{ fois}} \otimes \mathbf{C}^2$$

et donne un autre ket appartenant au même espace. C'est donc une matrice de dimensions $2^{n+1} \times 2^{n+1}$.

L'Oracle agit donc comme une porte *multicontrôle* (c.a.d qu'il y a plusieurs qubits de contrôle). Son circuit quantique est représenté sur la figure 6.2 Vérifions que l'on a bien à faire a une matrice *unitaire*. Pour cela il suffit de montrer qu'elle préserve le produit scalaire. Prenons deux vecteurs

$$U_f|x_1 \dots x_m, y\rangle \text{ et } U_f|x'_1 \dots x'_m, y'\rangle$$

et effectuons les produits scalaires :

$$\begin{aligned}
\langle x'_1 \dots x'_m, y'|U_f^\dagger U_f|x_1 \dots x_m, y\rangle &= \langle x'_1 \dots x'_m, y' \oplus f(x'_1 \dots x'_m)|x_1 \dots x_m, y \oplus f(x_1 \dots x_m)\rangle \\
&= \langle x'_1|x_1\rangle \dots \langle x'_m|x_m\rangle \langle y' + f(x'_1 \dots x'_m)|y + f(x_1 \dots x_m)\rangle \\
&= \delta_{x_1 x'_1} \dots \delta_{x_m x'_m} \langle y' + f(x'_1 \dots x'_m)|y + f(x_1 \dots x_m)\rangle \\
&= \delta_{x_1 x'_1} \dots \delta_{x_m x'_m} \delta_{y' y}
\end{aligned}$$

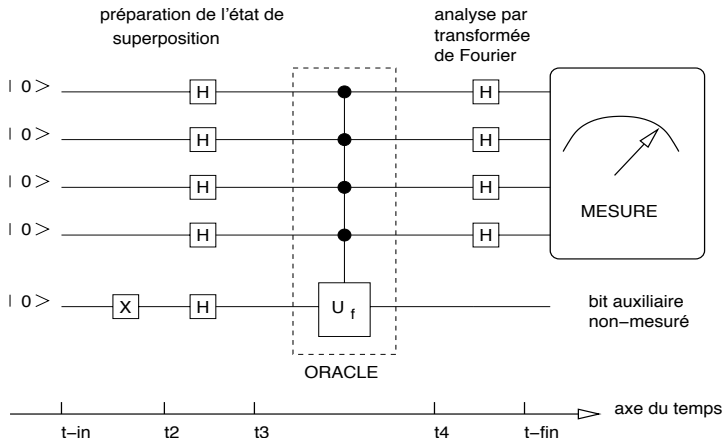


Figure 6.3 Circuit de l'algorithme de Deutsch-Jozsa

D'autre part

$$\begin{aligned}\langle x'_1 \dots x'_m, y'|x_1 \dots x_m, y\rangle &= \langle x'_1|x_1\rangle \dots \langle x'_m|x_m\rangle\langle y'|y\rangle \\ &= \delta_{x'_1 x_1} \dots \delta_{x'_m x_m}\delta_{y'y}\end{aligned}$$

6.6 Algorithme quantique de Deutsch-Jozsa

Pour chaque n on construit le circuit de la figure 6.3 L'algorithme est initialisé dans l'état (instant t_0).

$$\underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n \text{ fois}} \otimes |0\rangle = |\Psi_{in}\rangle$$

et se termine par une mesure dans la base computationnelle des n premiers qubits. Les projecteurs utilisés dans la mesure sont

$$P(b_1 \dots b_n) = |b_1 \dots b_n\rangle\langle b_1 \dots b_n|$$

Nous allons analyser l'évolution temporelle effectuée par un circuit aux instants t_{in}, t_2, t_3, t_{fin}. L'état final est donné par

$$|\Psi_{\text{fin}}\rangle = U(t_{\text{fin}}, t_{\text{in}})|\Psi_{in}\rangle = U(t_{\text{fin}}, t_4)U(t_4, t_3)U(t_3, t_2)U(t_2, t_{\text{in}})|\Psi_{in}\rangle$$

Les opérations d'évolution de chaque tranche sont

$$U(t_2, t_{\text{in}}) = (\underbrace{Id \otimes Id \otimes \cdots \otimes Id}_{n \text{ fois}}) \otimes X$$
$$U(t_3, t_2) = (\underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ fois}}) \otimes H$$
$$U(t_4, t_3) = U_f$$
$$U(t_{\text{fin}}, t_2) = (\underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ fois}}) \otimes Id$$

Etat à l'instant t_3.

$$\begin{aligned}
&\underbrace{(H \otimes H \otimes \cdots \otimes H)}_{n \text{ fois}} \otimes HX (\underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n \text{ fois}}) \otimes |0\rangle \\
&= (\underbrace{H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle}_{n \text{ fois}}) \otimes HX|0\rangle \\
&= \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) \otimes H|1\rangle \\
&= \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
&= \left(\frac{1}{2^{\frac{n}{2}}} \sum_{b_1 \ldots b_n} |b_1 \ldots b_n\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
\end{aligned}$$

A cet instant l'entrée est une *superposition cohérente de toutes les entrées classiques possibles*. Le dernier bit $\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$ est un bit auxiliaire qui va servir à stocker le résultat de l'Oracle.

Etat à l'instant t_4.

$$\begin{aligned}
&U_f \frac{1}{2^{\frac{n}{2}}} \sum_{b_1 \ldots b_n} |b_1 \ldots b_n\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - |1\rangle \right) \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{b_1 \ldots b_n} \left(\frac{1}{\sqrt{2}} U_f |b_1 \ldots b_n, 0\rangle - \frac{1}{\sqrt{2}} U_f |b_1 \ldots b_n, 1\rangle \right) \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{b_1 \ldots b_n} \left(\frac{1}{\sqrt{2}} |b_1 \ldots b_n, f(b_1 \ldots b_n)\rangle - \frac{1}{\sqrt{2}} |b_1 \ldots b_n, \overline{f(b_1 \ldots b_n)}\rangle \right)
\end{aligned}$$

Notons que si $f(b_1 \ldots b_n) = 0$ le terme entre parenthèses vaut

$$|b_1 \ldots b_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

et que si $f(b_1 \ldots b_n) = 1$ le terme entre parenthèses vaut

$$|b_1 \ldots b_n\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}}$$

On peut donc écrire l'état à l'instant t_4 comme suit:

$$\left(\frac{1}{2^{\frac{n}{2}}}\sum_{b_1\dots b_n}(-1)^{f(b_1\dots b_n)}|b_1\dots b_n\rangle\right)\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Cet état est à nouveau une superposition cohérente ou l'Oracle a déphasé chaque entrée classique de 0 à π suivant que[2] l'image de f est 0 ou 1.

Etat à l'instant t_{fin}. On applique finalement l'opérateur unitaire $\underbrace{H\otimes H\otimes\cdots\otimes H}_{n\text{ fois}}\otimes Id$,

ce qui donne par linéarité :

$$|\Psi_{\text{fin}}\rangle=\left(2^{\frac{n}{2}}\sum_{b_1\dots b_n}(-1)^{f(b_1\dots b_n)}H|b_1\rangle\otimes\cdots\otimes H|b_n\rangle\right)\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Notons que

$$H|b\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^b|1\rangle\right)=\frac{1}{\sqrt{2}}\sum_{c=0,1}(-1)^{cb}|c\rangle$$

si bien que

$$\begin{aligned}H|b_1\rangle\otimes\cdots\otimes H|b_n\rangle&=\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{b_1}|1\rangle\right)\otimes\cdots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{b_n}|1\rangle\right)\\&=\frac{1}{\sqrt{2}}\sum_{c_1=0,1}(-1)^{c_1b_1}|c_1\rangle\otimes\cdots\otimes\sum_{c_n=0,1}(-1)^{c_nb_n}|c_n\rangle\\&=\frac{1}{2^{\frac{n}{2}}}\sum_{c_1\dots c_n}(-1)^{\sum_{i=1}^n b_ic_i}|c_1\dots c_n\rangle\end{aligned}$$

Ainsi

$$|\Psi_{\text{fin}}\rangle=\sum_{c_1\dots c_n}\left\{\frac{1}{2^n}\sum_{b_1\dots b_n}(-1)^{f(b_1\dots b_n)}(-1)^{\sum_{i=1}^n b_1c_i}\right\}|c_1\dots c_n\rangle\otimes\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

L'état final est à nouveau une superposition cohérente d'états classiques affectés d'amplitudes

$$\frac{1}{2^n}\sum_{b_1\dots b_n}(-1)^{f(b_1\dots b_n)}(-1)^{\sum_{i=1}^n b_ic_i}$$

Les amplitudes contiennent de l'information sur la fonction f. Si nous les connaissions toutes nous pourrions en fait déterminer cette fonction. Mais la seule chose qui est à notre disposition est la totalité de l'état $|\Psi_{\text{fin}}\rangle$ (pris dans sa globalité) et *la seule chose que nous puissions faire, pour extraire de l'information, est une mesure.*

[2] Car $e^{\mathrm{i}0}=1$ et $e^{\mathrm{i}\pi}=-1$.

*

Dernière étape de l'algorithme: la mesure Appliquons le postulat de la mesure. Si nous mesurons l'état des n premiers qubits dans la base computationnelle$\{|c_1 \dots c_n\rangle, c_i = 0, 1\}$, l'état est projeté (ou réduit) sur *un* des états $|c_1 \dots c_n\rangle$ avec probabilité (règle de Born ou postulat de la mesure)

$$\begin{aligned}\text{Prob}(c_1 \dots c_n) &= [\text{carré de l'amplitude devant } |c_1 \dots c_n\rangle] \\ &= \frac{1}{2^{2n}} \left| \sum_{b_1 \dots b_n} (-1)^{f(b_1 \dots b_n)} (-1)^{\sum_{i=1}^n c_i b_i} \right|^2\end{aligned}$$

La signification de cette assertion est la suivante : tant que la mesure est faite une fois sur un unique état $|\Psi_{\text{fin}}\rangle$ l'état final observé est un des états $|c_1 \dots c_n\rangle$ et il n'y a aucun moyen de prédire lequel. Si l'on dispose d'un ensemble d'états $|\Psi_{\text{fin}}\rangle$, en répétant l'expérience plusieurs fois la fréquence des observations $|c_1 \dots c_n\rangle$ est donnée par $\text{Prob}(c_1 \dots c_n)$.

Calculons cette probabilité. Si f est constante on trouve

$$\begin{aligned}\text{Prob}(c_1 \dots c_n) &= \frac{1}{2^{2n}} \left| \sum_{b_1 \dots b_n} (-1)^{\sum_{i=1}^n c_i b_i} \right|^2 \\ &= \frac{1}{2^{2n}} \left| \sum_{b_1 \dots b_n} \prod_{i=1}^n (-1)^{c_i b_i} \right|^2 \\ &= \frac{1}{2^{2n}} \left| \prod_{i=1}^n \left((-1)^{c_i 0} + (-1)^{c_i 1} \right) \right|^2 \\ &= \begin{cases} 1 & \text{si } (c_1 \dots c_n) = (0 \dots 0) \\ 0 & \text{dans tous les autres cas} \end{cases}\end{aligned}$$

Donc si f est constante nous observerons certainement $(0 \dots 0)$ (c.a.d avec probabilité 1) en faisant une seule expérience ! Par contre si f est balancée on constate que

$$\text{Prob}(0 \dots 0) = \frac{1}{2^{2n}} \left| \sum_{b_1 \dots b_n} (-1)^{f(b_1 \dots b_n)} \right|^2 = 0$$

et on n'observera certainement pas $(0 \dots 0)$.

En conclusion : après le processus de mesure si $(0 \dots 0)$ est observé on peut conclure "f constante" et si autre chose est observé on peut conclure "f balancée". Remarquablement, il suffit de faire l'expérience et d'utiliser l'Oracle quantique une seule fois ! Ceci n'est pas typique des autres algorithmes quantiques: nous verrons par exemple que pour l'algorithme de Shor il faut faire l'expérience plusieurs fois pour amplifier la probabilité de succès.

Note sur la complexité de l'algorithme. En general nous devons distinguer la complexité du circuit et celle de l'algorithme proprement dit. Dans ce cours

la complexité des circuits sera mesurée en terme de deux grandeurs, la "profondeur" et la "largeur". La taille du circuit est alors définie comme le produit $(profondeur) \times (largeur)$. Ici le circuit contient 3 tranches de temps intermédiaires: on dit que ce circuit à une profondeur égale à 3 (ce qui est important ici c'est qu'elle est $O(1)$). Si le temps élémentaire requis pour effectuer une porte quantique (par RMN par ex) est de τ alors le temps de calcul du circuit est de 3τ. La largeur du circuit est donnée par le nombre de bits d'entrée plus le nombre de bits auxiliaires, ici $n+1$, et représente le nombre de calculs que le circuit quantique effectue à chaque tranche temporelle. La taille du circuit de DJ est donc $3(n+1) = O(n)$. Finalement quelle est la complexité de l'algorithme lui même ? Puisqu'on peut résoudre le problème de DJ en posant une seule question à l'Oracle, l'algorithme possède un temps de calcul $O(1)$ avec un circuit de taille $O(n)$.

6.7 Quelques remarques sur les réalisations expérimentales

Nous reviendrons sur les réalisations expérimentales à la fin du cours. Ce paragraphe peut être omis en première lecture.

L'algorithme de DJ fut un des premiers algorithmes quantique a être réalisé experimentalement (2001) pour le cas $n = 1$ par la résonance magnétique nucléaire. Cette experience utilise un liquide de $CHCl_3$ (le chloroforme, fig. 6.4). Pour $n = 1$ il faut deux bits quantiques, un pour l'entrée et un bit auxiliare pour stocker le résultat de l'Oracle. Ceux-ci sont matérialisés par les spins nucléaires de l'atome d'hydrogène H et de carbone C. Les portes de Hadamard et l'Oracle peuvent être réalisés en manipulant ces deux spins nucléaires par des champs magnétiques de radiofréquence. Un des problèmes principaux est de préparer toutes les molécules du liquide dans l'état initial $|00\rangle$. En effet on ne peut pas se débarasser complètement des fluctuations thermiques qui induisent des transitions vers les autres états pour une fraction des molécules du liquide. Pour augmenter n il faut prendre de plus grosses molécules avec des atomes appropriés. Ceci pose un problème ("scalability problem") parceque plus la molecule est grosse plus les niveaux d'énergie sont nombreux et rapprochés (le spectre devient continu en quelque sorte) et il devient de plus en plus difficile de manipuler sélectivement les bits quantiques grâce à des transitions de radiofréquence. Plus récemment, l'agorithme de DJ a aussi été réalisé grâce aux technologies des pièges à ions et des cavités resonantes (cavity QED). Toutes ces experiences sont limitées à un faible nombre de qubits (< 10 qubits).

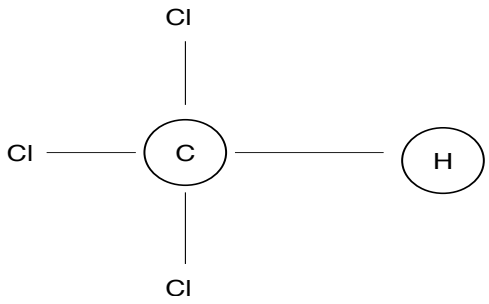


Figure 6.4 L'algorithme DJ a été réalisé par Résonance Magnétique Nucléaire sur les molécules de $CHCl_3$. On agit sur deux qubits associés aux spins nucléaires des atomes H et C entourés

7 Factorisation et Algorithme de Shor

Un des développements les plus spectaculaires du calcul quantique est l'algorithme de Shor. Il s'agit d'un algorithme de factorisation pour les entiers de complexité polynomiale dans la taille de l'entier.

Le théorème fondamental de l'arithmétique nous assure que tout entier N peut être décomposé de facon unique en un produit de nombres premiers. étant donné les facteurs de N, il est facile de vérifier que le produit de ces facteurs redonne N. Plus précisément supposons que $N = p \cdot q$ avec p et q deux nombres premiers à Ob bits. Si p et q sont connus, la vérification $N = p \cdot q$ peut se faire facilement avec Ob^2 opérations. Par contre étant donné un entier général N avec Ob bits on ne connaaît pas d'algorithme polynomial permettant de calculer p et q (on ne sait même pas s'il en existe un ou non). On connaît plusieurs algorithmes plus rapides que $O(1+\epsilon)^b$ pour tout $\epsilon > 0$. Le meilleur algorithme connu possède un temps de calcul $O\exp(\frac{64}{9}b)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}$. Concrètement un des records[1] relativement récents de factorisation atteint le 12 décembre 2009 pour un nombre à 232 décimales (b=768 bits) a utilisé des centaines de processeurs sur deux années de calcul.

Comme nous le verrons plus tard, l'algorithme de Shor permet une factorisation en temps polynomial avec un circuit quantique de taille polynomiale. L'algorithme de Shor résoud en fait un autre problème de théorie des nombres appelé *la recherche de l'ordre*. Il est connu depuis 1976 (environ) que la factorisation peut se réduire à la recherche de l'ordre.

Pour analyser la compexité de l'algorithme de Shor nous aurons aussi besoin de quelques notions supplémentaires sur les fractions continuées et la fonction d'Euler. Celles-ci ainsi que la réduction de la factorisation à la recherche de l'ordre sont exposées dans la section suivante.

7.1 Une parenthèse de théorie de nombres

Factorisation basée sur la recherche de l'ordre

Soit $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ avec $p_i \neq 2$ et $k \geq 2$. En d'autres termes N ne contient pas de puissance de 2 et N n'est pas la puissance d'un nombre premier unique ($N \neq p^e$). Notez que les puissances de 2 sont aisément extraites car il est facile

[1] Voir http://en.wikipedia.org/wiki/RSA_numbers#RSA-768

de voir si un entier et pair et de diviser par 2. De plus si $N = p^e$ il existe une méthode efficace pour trouver p et e.

Algorithme de factorisation basé sur la recherche de l'ordre.

a. Choisir aléatoirement uniformément $a \in \{2, \cdots, N-1\}$ et calculer

$$d = \text{PGCD}a, N$$

grâce à l'algorithme d'Euclide (de complexité $O((\log_2 N)^3)$).

b. Si $d > 1$ nous avons un facteur non-trivial de N car $d|N$, (d divise N). On garde ce facteur et on retourne à a.

c. Si $d = 1$ (c'est-à-dire que a et N sont premiers entre eux) on calcule *le plus petit* entier r tel que

$$a^r = 1 \mod N.$$

Cet entier s'appelle *l'ordre de* $a \mod N$ aussi noté $r = \text{Ord}_N(a)$. *Pour cette étape on ne connaaît pas d'algorithme classique polynomial. C'est l'étape qui sera traitée par l'algorithme de Shor.*

d. Supposons que r soit impair. Output `Fail` et retourner à a.

e. Si r est pair alors on sait que

$$a^r - 1 = \left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)$$

Notez que N divise $a^r - 1$. Donc il y a a priori 3 possibilités:

e1. N divise $a^{\frac{r}{2}} - 1$. Ceci est en fait impossible car alors on aurait $a^{\frac{r}{2}} = 1 \mod N$ et $\frac{r}{2}$ serait l'ordre.

e2. N divise $a^{\frac{r}{2}} + 1$. C'est-à-dire $a^{\frac{r}{2}} = -1 \mod N$. Output `Fail` et retourner à a.

e3. N partage des facteurs non-triviaux avec $a^{\frac{r}{2}} - 1$ et $a^{\frac{r}{2}} + 1$. Par exemple si $N = pq$ il faut que $p|(a^{\frac{r}{2}} - 1)$ et $q(|a^{\frac{r}{2}} + 1)$ ou vice versa. En d'autres termes

$$d_\pm = \text{PGCD}a^{\frac{r}{2}} \pm 1, N$$

sont non-triviaux $d_+ > 1$ et $d_- > 1$ et nous avons 2 facteurs non-triviaux de N. Ceux-ci sont calculés grâce à l'algorithme d'Euclide (Complexité $O(\log_2 N)^3$).

f. Vérifier si le produit des facteurs trouvés dans les étapes précédentes vaut N. Si ce n'est pas encore le cas retourner à a.

Nous voyons qu'en présence d'un oracle qui permettrait résoudre l'étape c. la complexité d'une expérience (un round) provient uniquement de l'algorithme d'Euclide qui est Ob^3. Néanmoins cette expérience est probabiliste (étape a) et nous devons nous assurer que la probabilité de succès est non-négligeable. En fait on peut prouver $\mathbb{P}[\text{succès}] \geq \frac{3}{4}$. Cela implique qu'avec $T = \frac{|\ln \epsilon|}{|\ln 2|}$ expériences

(rounds) on peut amplifier cette probabilité de succès à $\mathbb{P}\left[\text{succès en T rounds}\right] \geq 1-\epsilon$.

Lors d'un round les seuls output `Fail` interviennent en d. et e2. Cela correspond à l'évènement

$$(r \text{ est impair}) \text{ ou } (a^{\frac{r}{2}} = -1 \mod N)$$

Ainsi

$$\mathbb{P}\left[\text{échec}\right] = \mathbb{P}\left[(r \text{ est impair}) \text{ ou } (a^{\frac{r}{2}} = -1 \mod N)\right].$$

Théorème. Soit a pris uniformément aléatoirement dans $2, \cdots, N-1$. Soit r les plus petit entier satisfaisant à $a^r = 1 \mod N$. Alors $\mathbb{P}\left[\text{échec}\right] \leq \frac{1}{4}$.

Nous ne donnons pas de preuve ici. Ce théorème assure que la probabilité de succès de l'algorithme de factorisation basé sur la recherche de l'ordre est d'au moins $\frac{3}{4}$ lors d'un seul round. En faisant des ronds successifs il est possible d'amplifier cette probabilité à $1-\epsilon$ ($\epsilon \ll 1$). Comme d'habitude le nombre de rounds requis est de l'ordre de $O|\ln \epsilon|$.

Fractions continuées

Dans ce paragraphe nous donnons, sans démonstration, quelques résultats de théorie des nombres, utiles pour le développement ultérieur de l'algorithme de Shor.

Tout nombre réel peut être développé en *fraction continuée*. Ici nous discutons ce processus uniquement pour les *fractions rationnelles*. Prenons un exemple. Soit la fraction $x = \frac{263}{189}$. Les étapes succesives de l'algorithme d'Euclide du calcul du PGCD$263, 189$ sont:

$$\begin{aligned} 263 &= 1 \cdot 189 + 74 \\ 189 &= 2 \cdot 74 + 41 \\ 74 &= 1 \cdot 41 + 33 \\ 41 &= 1 \cdot 33 + 8 \\ 33 &= 4 \cdot 8 + 1 \end{aligned}$$

On voit que PGCD$263, 189 = 1$. Etant donné qu'à chaque fois on divise par un nombre ≥ 2 le nombre d'étapes (de lignes ci-dessus) est de l'ordre de $\log_2(263)$, c'est-à-dire $\log_2(N)$ en général. De plus, chaque division requiert $O(\log_2 N)^2$ opérations. Donc le nombre total d'opérations pour l'algorithme d'Euclide est $O(\log_2 N)^3$. Maintenant, pour obtenir le *développement en fraction continuée*, on procède de la sorte:

$$\frac{263}{189} = 1 + \frac{74}{189} = 1 + \frac{1}{\frac{189}{74}} = 1 + \frac{1}{2 + \frac{41}{74}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{\cfrac{74}{41}}} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{33}{41}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\cfrac{41}{33}}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{8}{33}}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{33}{8}}}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{8}}}}}$$

On dit que le développement en fraction continue est

$$\frac{263}{189} = [1; 2; 1; 1; 4; 8]$$

La forme générale du développement est :

$$x = [a_0; a_1; \cdots ; a_n]$$

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Si $x > 1$ on a $a_0 \geq 1$ et si $x < 1$ on a $a_0 = 0$. De plus, ce développement n'est pas unique car on peut toujours écrire le dernier terme $\frac{1}{a_n}$ comme $\frac{1}{(a_n-1)+\frac{1}{1}}$. Ainsi

$$x = [a_0; a_1; \cdots a_{n-1}; a_n] = [a_0; a_1; \cdots ; a_{n-1}; a_n - 1; 1]$$

Mais à cette ambigüité près le développement est unique. De plus on peut le rendre unique en déclarant que l'on choisit toujours le développement le plus court possible. Le nombre d'opérations requises est le même que pour l'algorithme d'Euclide, $O(\log_2 N)^3$ ou $N = \max$(numérateur, dénominateur). La longueur du développement est $O(\log_2 N)$.

Définition: Notion de Convergent. Soit $x = [a_0; a_1; a_2; \cdots ; a_n]$ un développement en fraction continuée de x. On appelle *convergents* les séries tronquées $[a_0; a_1; a_2; \cdots ; a_m]$, $1 \leq m \leq n$. Ces convergents sont des nombres rationnels

$$[a_0; a_1; a_2; \cdots ; a_m] = \frac{p_m}{q_m}.$$

Théorème: Propriétés des Convergents. Soit p_m/q_m l'ensemble des convergents d'une fraction x. Alors

a) PGCD$p_m, q_m = 1$ (p_m et q_m sont premiers entre eux) et
$\left|x - \frac{p_m}{q_m}\right| \leq \frac{1}{q_m^2}$ (les convergents forment de bonnes approximations).

b) Réciproquement, toutes les approximations de la forme p/q avec p et q premiers entre eux, telles que $\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$ sont données par l'ensemble des convergents de x. On peut donc calculer ces approximations de facon systématique.

Pour nous, c'est la propriété b) qui sera utile dans l'analyse de l'algorithme de Shor.

Exercice: Donnez la liste de tous les convergents de $x = \frac{263}{189}$ et vérifiez l'affirmations (a) du théorème..

Fonction d'Euler

Pour un entier $r > 2$ on dit que $a \in \{1, 2, 3, \ldots, r-1\}$ est premier avec r (a is coprime with r) si PGCD$a, r = 1$. Le nombre de tels entiers a est donné par $\varphi(r)$, la *fonction d'Euler*. Si N est premier, $N = p$ on a bien sur : $a = 1, 2, 3, \ldots, p-1$ et $\varphi(p) = p - 1$. En général on montre que si

$$N = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

est la décomposition (unique) en facteurs premiers de N,

$$\begin{aligned}\varphi(N) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \ldots \varphi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\ldots p_k^{e_k-1}(p_k-1)\end{aligned}$$

Exemple. Si $N = 9$ les a premiers avec N sont $a = 1, 2, 4, 5, 7, 8$ et donc $\varphi(9) = 6$. On vérifie $\varphi(9) = 3^{2-1}(3-1) = 6$

L' inégalité suivante (valable pour r assez grand) sera utile pour nous:

$$\varphi(r) \geq \frac{r}{4 \ln \ln r}$$

Le dénominateur $\ln \ln r$ croît extrêmement lentement. Par exemple pour $r = 10^{1000}$ (ce qui représente un nombre à 1000 décimales) on a $\ln \ln r = \ln(1000 \ln 10) = 3 \ln 10 + \ln \ln 10 \leq 8$. En d'autre termes, étant donné r, une fraction appréciable des $r-1$ nombres inférieurs sont premiers avec r (dans l'exemple cette fraction est supérieure à $1/32$). Cette propriété peut être ré-exprimée comme suit. Fixons r et tirons $k \in \{1, 2, \ldots, r\}$ au hasard, uniformément, (c.a.d avec probabilité $\frac{1}{r}$. Alors:

$$\mathbb{P}\left[\text{PGCD}k, r = 1\right] = \frac{\varphi(r)}{r} \geq \frac{1}{4(\ln \ln r)}$$

Le membre de droite de l'inégalité décroît très lentement: on pourra y penser comme étant $O(1)$ (même si cela n'est pas vrai bien sûr!).

7.2 Recherche de la période d'une fonction arithmétique

Comme nous l'avons expliqué, on peut ramener la factorisation d'un entier N à la recherche de l'ordre d'un nombre a pris au hasard dans $\{2, 3, ..., N-1\}$. L'ordre $Ord_n(a)$ est le plus petit entier r tel que

$$a^r = 1 \mod N.$$

En d'autres termes, nous cherchons la période de la fonction arithmétique

$$\begin{aligned} f_{a,N} &: \mathbb{Z} \to \mathbb{Z} \\ & x \to f_{a,N}(x) = a^x \mod N. \end{aligned}$$

Cette période (ou l'ordre) est le plus petit entier r t.q.

$$f_{a,N}(x) = f_{a,N}(x + r), \qquad \forall x \in \mathbb{Z}.$$

Nous commencons donc par étudier un algorithme général de "recherche de la période d'une fonction arithmétique".

Soit $f : \mathbb{Z} \to \mathbb{Z}$ de période inconnue

$$f(x) = f(x + r), \qquad \forall x \in \mathbb{Z}.$$

Comme nous serons obligés de travailler avec un nombre fini de bits, nous allons tronquer $\mathbb{Z}$ á $\frac{\mathbb{Z}}{M\mathbb{Z}} = \{0, 1, 2, ...M-1\}$ où M est choisi bien plus grand que r : $M >> r$. Ici, $\frac{\mathbb{Z}}{M\mathbb{Z}}$ est le groupe additif des entiers pris $\mod M$. En fait r est inconnu, mais nous supposons que l'on connait une borne supérieure, et qu'il est donc possible de choisir $M >> r$. Par exemple, pour la recherche de l'ordre, nous

savons que $r < N$. Nous verrons dans ce cas que $M = O(N^2)$ est suffisant.

Tout d'abord il nous faut représenter les entiers $x \in \{0, ..., M-1\}$ par des états quantiques. Nous prenons (sans perte de généralité) $M = 2^m$ et notons que x peut être représenté grâce à son expansion binaire

$$x = 2^{m-1}x_{m-1} + 2^{m-2}x_{m-2} + ... + 2^2x_2 + 2x_1 + x_0,$$

avec m bits

$$x = \underbrace{(x_{m-1}.....x_0)}_{\text{dev binaire de x}}.$$

En particulier $(0, ..., 0) = 0$ et $(1, ..., 1) = 2^m - 1$. Il est donc naturel de prendre comme espace de Hilbert

$$\mathcal{H} = \underbrace{C^2 \otimes C^2 \otimes ... \otimes C^2}_{\text{m fois}},$$

et de stocker l'entier x dans un état quantique $|x\rangle \in \mathcal{H}$ construit à partir de m qubits (m systèmes à 2 niveaux: spins nucléaire, polarisation des photons...)

$$|x\rangle = |x_{m-1}\rangle \otimes ... \otimes |x_0\rangle = |x_{m-1}, ..., x_0\rangle.$$

La fonction f est comme d'habitude représentée par l'opération unitaire

$$U_f : |x\rangle \otimes |0\rangle \to U_f|x\rangle \otimes |0\rangle = |x\rangle \otimes |f(x)\rangle$$

où $|0\rangle$ et $|f(x)\rangle$ dont des états à m qubits (dans l'algorithme de shor on calcule $f(x)$ mod N et donc m bits suffisent certainement). Nous aurons aussi besoin de la "Transformée de Fourrier Quantique" définie par :

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} |y\rangle \quad = \frac{1}{2^{m/2}} \sum_{y_0....y_{m-1} \in \{0,1\}^m} e^{2\pi i \frac{xy}{M}} |y_0....y_{m-1}\rangle$$

Cette opération est linéaire c.a.d que si $|Psi\rangle = \sum_{x=0}^{M-1} c_x|x\rangle$, alors

$$QFT|Psi\rangle = \sum_{x=0}^{M-1} c_x QFT|x\rangle.$$

On peut aussi montrer que l'opération est unitaire : ceci est un prérequis important pour pouvoir la réaliser grâce à un circuit quantique.

7.3 Circuit pour la recherche de la période

Le circuit de l'algorithme de recherche de la période est représenté sur la figure 10.7.

Le circuit pour U_f dépend de la fonction spécifique. Pour la recherche de l'ordre

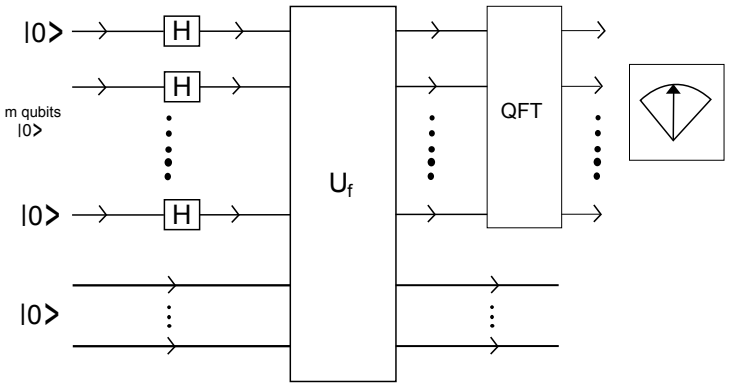


Figure 7.1 Circuit quantique pour la recherche de la période d'une fonction arithmétique

nous prendrons la fonction $f(x) = a^x \mod N$ et verrons comment réaliser son circuit au paragraphe 7.7. Le circuit pour QFT sera réalisé au paragraphe 7.6.

Calculons maintenant l'évolution de l'état initial :

$$|0\rangle \otimes |0\rangle = \underbrace{|0...0\rangle}_{\text{m fois}} \otimes \underbrace{|0...0\rangle}_{\text{m fois}}.$$

Juste après les portes de Hadamard :

$$H^{\otimes m} \underbrace{|0...0\rangle}_{\text{m fois}} \otimes |0\rangle ... = \left(\frac{1}{2^{\frac{m}{2}}} \sum_{x_0 ... x_{m-1} \in \{0,1\}^m} |x_{m-1} .... x_0\rangle \right) \otimes |0\rangle.$$

C'est un état de superposition cohérente sur toutes les entrées classiques. Il peut aussi s'écrire de facon plus compacte:

$$\left(\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \right) \otimes |0\rangle.$$

Après U_f nous obtenons l'état

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle.$$

Exploitons le fait que f est périodique pour réorganiser cette somme. L'intervalle $[0, M-1]$ est décomposé en morceaux de longueur r, sauf pour le dernier qui sera plus court. Les entiers dans la premiere periode sont $x_0 \in \{0, 1, ..., r-1\}$. Si M était un multiple de r, on pourrait représenter chaque x comme

$$x = x_0 + jr \text{ avec } 0 \leq j \leq \frac{M}{r} - 1.$$

Dans le cas général (voir figure 7.2) on aura

$$x = x_0 + jr \text{ avec } 0 \leq j \leq A(x_0) - 1,$$

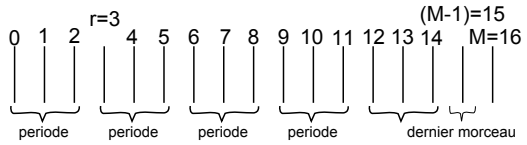


Figure 7.2 Exemple de décomposition de $\{0, 1, ..., M-1\}$ pour $r = 3$ et $M = 16$

et $A(x_0)$ un entier dépendant de x_0 qui doit satisfaire

$$M - r \leq x_0 + (A(x_0) - 1)r \leq M - 1.$$

Nous avons :

$$\begin{aligned}\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0 + jr)\rangle \\ =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0)\rangle.\end{aligned}$$

Finalement nous agissons sur cet état avec QFT. L'état obtenu est :

$$\begin{aligned}|Psi_{\text{fin}}\rangle =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} QFT|x_0 + jr\rangle \otimes |f(x_0)\rangle \\ =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{(x_0+jr)y}{M}} |y\rangle \otimes |f(x_0)\rangle \\ =& \frac{1}{M} \sum_{x_0=0}^{r-1} \left(\sum_{y=0}^{M-1} \left(e^{2\pi i \frac{x_0 y}{M}} \sum_{j=0}^{A(x_0)-1} e^{2\pi i \frac{jy}{M/r}} \right) |y\rangle \right) \otimes |f(x_0)\rangle.\end{aligned}$$

Cette dernière expression est l'état final $|Psi_{\text{fin}}\rangle$ juste avant la mesure.

7.4 Le Processus de Mesure

Il reste maintenant à analyser l'opération de mesure. Tout d'abord il nous faut choisir une "base représentant l'appareil de mesure". Celle-ci est formée par l'ensemble des projecteurs.

$$P_y = |y\rangle\langle y| \otimes \mathbb{I}_{m \times m}, \qquad y \in \{0, 1, 2, \cdots M-1\}.$$

L'état quantique résultant juste après la mesure est (à une normalisation près)

$$P_y |Psi\rangle_{\text{fin}}$$

avec la probabilité

$$\text{Prob}(y) = \langle \Psi_{\text{fin}} | P_y | \Psi_{\text{fin}} \rangle.$$

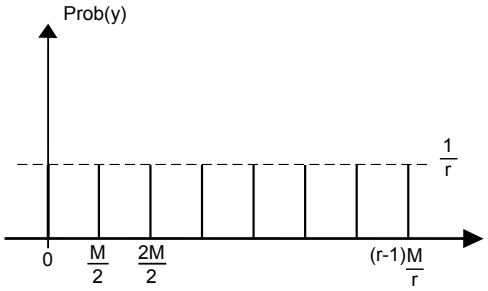


Figure 7.3 Distribution de probabilité des résultats de mesures pour M multiple de r.

D'abord, on calcule $P_y|Psi_{\mathrm{fin}}\rangle$,

$$P_y|Psi_{\mathrm{fin}}\rangle == \frac{1}{M}\sum_{x_0=0}^{r-1}\left(e^{2\pi i\frac{x_0 y}{M}}\sum_{j=0}^{A(x_0)-1}e^{2\pi i\frac{jy}{M/r}}\right)|y\rangle\otimes|f(x_0)\rangle.$$

Puis $\langle\Psi_{\mathrm{fin}}|P_y|\Psi_{\mathrm{fin}}\rangle = \langle\Psi_{\mathrm{fin}}|P_yP_y|\Psi_{\mathrm{fin}}\rangle$. Cela donne

$$\mathrm{Prob}(y) = \frac{1}{M^2}\sum_{x_0=0}^{r-1}\left|\sum_{j=0}^{A(x_0)=1}e^{2\pi i\frac{jy}{M/r}}\right|^2.$$

Remarquons que les différents termes de la somme sur x_0 n'interfèrent pas car les kets $|f(x_0)\rangle$ sont orthogonaux entre eux.

7.5 Analyse de la probabilité $\mathrm{Prob}(y)$

Traitons d'abord le cas (irréaliste) simple ou M serait multiple de r

Dans ce cas, $A(x_0) = \frac{M}{r}$ et donc

$$\mathrm{Prob}(y) = \frac{r}{M^2}\left|\sum_{j=0}^{\frac{M}{r}-1}e^{2\pi i\frac{jy}{M/r}}\right|^2.$$

Si $y = k\frac{M}{r}$ avec $k = \{0, 1, ..., r-1\}$ on a

$$e^{2\pi i\frac{jy}{M/r}} = e^{2\pi ijk} = 1.$$

Si bien que $\mathrm{Prob}(y) = \frac{r}{M^2}\left|\frac{M}{r}\right|^2 = \frac{1}{r}$. Puisque cette probabilité doit se sommer à 1, nous en déduisons qu'elle est nulle pour toutes les autres valeurs de $y \neq k\frac{M}{r}$. Cette distribution est représentée sur la figure 7.3.

La mesure donne avec probabilité 1 une valeur de y de la forme

$$y = k\frac{M}{r} \;\; avec \;\; k \in \{0, 1, ..., r-1\}.$$

Puisque M est connu, grâce à la valeur de y donnée par la mesure, nous calculons $\frac{y}{M}$. Deux cas de figure se presentent à nous:

- $\frac{y}{M} = \frac{k}{r}$ et PGCD$k, r = 1$. Alors nous pouvons trouver k et r en simplifiant la fraction $\frac{y}{M}$ "au maximum" jusqu'à ce que les numérateurs et dénominateurs n'aient plus de facteurs communs. Nous trouvons ainsi r.
- $\frac{y}{M} = \frac{k}{r}$ et PGCD$k, r \neq 1$. Alors nous ne savons pas jusqu'où simplifier la fraction (et n'avons pas de facon systématique de trouver k et r).

En "pratique" nous ne savons pas à priori si k et r sont premiers entre eux ou non. Ainsi nous adoptons la procédure suivante: dans tous les cas simplifier la fraction $\frac{y}{M}$ au maximum, et tester si le r trouvé est une période de $f(x)$ ou non.

La probabilité de succès est la probabilité d'avoir PGCD$k, r = 1$ quand k est tiré uniformément dans $\{0, 1, ..., r-1\}$. D'après ce que nous avons appris dans le chapitre précédent:

$$\text{Prob}(\text{PGCD}k, r = 1, k \in \{0, 1, ..., r-1\}) = \frac{\varphi(r)}{r} \geq \frac{1}{4(\ln \ln r)}.$$

Puisque $r < M$, nous avons *une probabilité de succès pour une expérience*:

$$\text{Prob}(\text{succes}) \geq \frac{1}{4 \ln \ln\, M} \qquad \left(= \frac{1}{4 \ln 2 \ln m}\right).$$

Bien que cette probabilité soit faible, nous pouvons l'amplifier en faisant tourner le circuit plusieurs fois. Au bout de T expériences (ou "rounds"):

$$\text{Prob}(\text{au moins 1 succes au bout de T rounds}) \geq 1 - \left(1 - \frac{1}{4 \ln \ln\, M}\right)^T,$$

ce qui peut être rendu proche de $1 - \epsilon$ si on prend

$$T = O(|\ln \epsilon| \ln \ln\, M) = O(|\ln\, m||\ln \epsilon|).$$

En effet:

$$\begin{aligned}
&1 - \left(1 - \frac{1}{4 \ln\, M}\right)^T \geq 1 - \epsilon \\
&\leftrightarrow \epsilon \geq \left(1 - \frac{1}{4 \ln\, M}\right)^T \leftrightarrow \ln \epsilon \geq T \ln \left(1 - \frac{1}{4 \ln\, M}\right) \\
&\leftrightarrow \ln \epsilon \geq -T \frac{1}{4 \ln\, M} \ (M \text{ grand}) \\
&\leftrightarrow T \geq 4(\ln \ln\, M)|\ln \epsilon|
\end{aligned}$$

Passons maintenant au cas général ou M n'est pas un multiple de r.

Nous allons utiliser un Lemme technique (la démonstration n'est pas donnée ici). Une illustration graphique de son contenu est fournie par la figure 7.4. En gros,

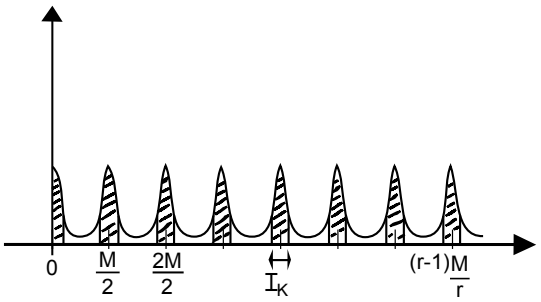


Figure 7.4 Distribution de probabilité fournie par les mesures. L'aire hachurée est superieure a $\frac{2}{5}$. Notez que les intervalles I_k ont une longueur 1 et sont distant d'environ $M/r >> 1$.

le Lemme affirme que la distibution de probabilité $\mathrm{Prob}(y)$ est concentrée sur les entiers proches des fractions kM/r.

Lemme. Soit $I = \cup_{k=0}^{r-1}\left[k\frac{M}{r} - \frac{1}{2}, k\frac{M}{r} + \frac{1}{2}\right] = \cup_{k=0}^{r-1} I_k$ une union d'intervalles disjoints I_k. Alors,

$$\mathrm{Prob}(y \in I) \geq \frac{2}{5}.$$

Ainsi, avec probabilité au moins $\frac{2}{5}$ les mesures fournissent des entiers y proches de $k\frac{M}{r}$ avec $k \in \{0, 1, ..., r-1\}$. Lorsqu'une mesure donne $y \in I$ cela signifie qu'il existe k entier tel que

$$k\frac{M}{r} - \frac{1}{2} \leq y \leq k\frac{M}{r} + \frac{1}{2},$$

ce qui est équivalent à

$$\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2M}. \tag{7.1}$$

Maintenant supposons que nous prenions $M > r^2$. Alors cette inégalité entraine,

$$\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2r^2} \text{ pour } k \in \{0, 1, ..., r-1\}.$$

Comment pouvons nous determiner k et r à partir de y et M ? D'après ce que nous avons vu dans la théorie des fractions continuées, si le PGCD$k, r = 1$, alors $\frac{k}{r}$ est nécessairement un "convergent" du développement en fractions continuées de $\frac{y}{M}$. Il y a un nombre fini de "convergents" car $\frac{y}{M}$ est rationnel, et ceux-ci peuvent être systématiquement calculés grâce à l'algorithme d'Euclide (en temps $O((\ln M)^3)$. Par contre si PGCD$k, r \neq 1$ on ne peut pas affirmer que $\frac{k}{r}$ est un convergent de $\frac{y}{M}$ et n'avons, dans ce cas, pas de moyen systématique de calculer k et r.

Nous adoptons donc la procédure suivante. Nous calculons tous les convergents de $\frac{y}{M}$ (grâce à l'algorithme d'Euclide) et examinons leurs dénominateurs r. Pour

chacun de ces dénominateurs nous testons si c'est une période de $f(x)$. Le succès est assuré si PGCD$k, r = 1$, ce qui a lieu avec probabilté $O(\frac{1}{4 \ln \ln r})$.

Récapitulons. Quel est la probabilité de succès lors d'une expérience avec le circuit quantique ? Le circuit quantique est initialisé dans l'état $|0\rangle \otimes |0\rangle$. L'evolution unitaire conduit à l'état $|Psi_{\text{final}}\rangle$, après quoi on effectue une mesure. Cette mesure donne l'entier y. Pour en déduire r avec succès, il faut remplir deux conditions:

- $y \in I$ pour un certain $k \in \{0, 1, ..., r-1\}$.
- Etant donné $y \in I_k$ il faut PGCD$k, r = 1$.

Donc:

$$\text{Prob(succes)} \geq \frac{2}{5} \times \frac{1}{4 \ln \ln r}.$$

En itérant l'experience $T \approx O(|\ln \epsilon| \ln \ln r)$ fois on peut amplifier la probabilité de succès à $1 - \epsilon$.

7.6 Le circuit de la QFT

Dans ce paragraphe nous montrons comment réaliser le circuit de la QFT. En exercice nous avons vu que pour $M = 2$, on a $QFT = H$ (la porte de Hadamard):

$$(QFT)_{M=2}|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle).$$

Pour $M = 4$,

$$\begin{aligned}(QFT)_{M=4}|x\rangle &= \frac{1}{\sqrt{4}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle + e^{i\pi x}|2\rangle + e^{3i\frac{\pi}{2}x}|3\rangle\right) \\ &= \frac{1}{\sqrt{4}}\left(|00\rangle + e^{i\frac{\pi}{2}x}|01\rangle + e^{i\pi x}|10\rangle + e^{3i\frac{\pi}{2}x}|11\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi x}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle\right).\end{aligned}$$

En notation binaire $x \in \{0, 1, 2, 3\}$ est représenté par

$$x = 2x_1 + x_0\,;\; x_0, x_1 \in \{0, 1\}$$

si bien que $e^{i\pi x} = e^{2\pi i x_1} e^{i\pi x_0} = (-1)^{x_0}$ et $e^{i\frac{\pi}{2}x} = e^{i\pi x_1} e^{i\frac{\pi}{2}x_0} = (-1)^{x_1} e^{i\frac{\pi}{2}x_0}$. On trouve alors

$$(QFT)_{M=4}|x\rangle = \left(\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + (-1)^{x_1} e^{i\frac{\pi}{2}x_0}|1\rangle}{\sqrt{2}}\right).$$

Cette factorisation est à la base de la réalisation du circuit de la QFT. La factorisation suggère le circuit suivant de la figure 7.5. La première opération $SWAP$ échange les deux qubits. Elle peut être réalisée par trois portes $CNOT$ (figure 7.6). La seconde operation de la figure 7.5 est une porte de Hadamard

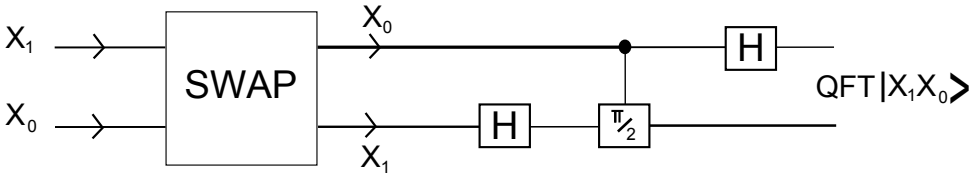


Figure 7.5 Circuit de la $(QFT)_{M=4}$.

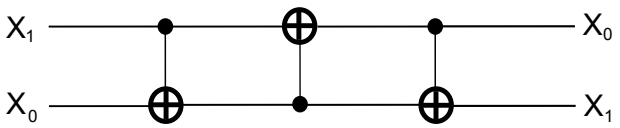


Figure 7.6 Circuit pour un $SWAP$.

agissant sur $|x_1\rangle$ pour produire $\frac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_1}|1\rangle)$. La troisième opération est un "phase shift" controlé par le premier bit x_0: si $x_0 = 0$ il n'y a pas de phase shift et le second bit reste dans l'etat $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$; par contre si $x_0 = 1$, il y a un phase shift et le second bit est transformé en $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}e^{i\frac{\pi}{2}}|1\rangle)$. Enfin, la dernière porte de Hadamard agit sur $|x_0\rangle$ pour produire $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0}|1\rangle)$.

Le circuit général de la QFT est obtenu par une généralisation des remarques ci-dessus.

Lemme. Pour $x \in \{0, 1, ...M-1\}$ et $M = 2^m$

$$QFT|x\rangle = \prod_{l-1}^{m} \frac{(|0\rangle + e^{i\frac{\pi}{2^{l-1}}x}|1\rangle)}{\sqrt{2}}.$$

Démonstration. Rappelons que

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}}|y\rangle = \frac{1}{2^{\frac{m}{2}}} \sum_{y=0}^{2^m-1} e^{2\pi i \frac{xy}{2^m}}|y\rangle.$$

Chaque $y \in \{0, 1, ..., 2^m - 1\}$ possède un developpement binaire

$$\begin{aligned} y &= 2^{m-1}y_{m-1} + 2^{m-2}y_{m-2} + ... + 2y_1 + y_0 \\ &= 2y' + y_0 \end{aligned}$$

où $y' = 2^{m-2}y_{m-1} + ... + y_1$. On décompose la somme sur y en une somme avec $y_0 = 0$ et une somme avec $y_0 = 1$ (cela revient a séparer les y pairs et impairs.)

$$\begin{aligned} QFT|x\rangle &= \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x2y'}{2^m}}|y'\rangle \otimes |0\rangle + \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x(2y'+1)}{2^m}}|y'\rangle \otimes |1\rangle \\ &= \left(\frac{1}{2^{\frac{m-1}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{xy'}{2^{m-1}}}|y'\rangle\right) \otimes \left(|0\rangle + e^{\frac{\pi i x}{2^{m-1}}}|1\rangle\right). \end{aligned}$$

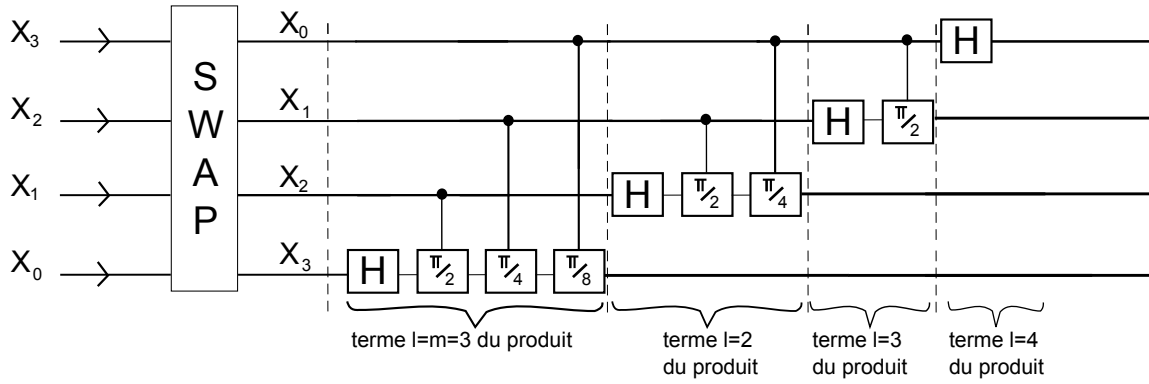


Figure 7.7 Circuit de la QFT pour 4 qubits.

Cette factorisation peut maintenant être répétée sur la premiere parenthèse. La seule difference est que $m \to m-1$. On obtient

$$QFT|x\rangle = \left(\frac{1}{2^{\frac{m-2}{2}}} \sum_{y''=0}^{2^{m-2}-1} e^{2\pi i \frac{xy''}{2^{m-2}-1}} |y''\rangle \right) \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-2}}}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-1}}}|1\rangle}{\sqrt{2}}.$$

En itérant ce procédé, on obtient le résultat du lemme.

La dernière étape consiste à remplacer x par son développement binaire (comme nous l'avons fait pour $M = 4$)

$$x = 2^{m-1}x_{m-1} + ... + 2^2 x_2 + 2x_1 + x_0,$$

ce qui implique pour tout $1 \leq l \leq m$

$$e^{i\frac{\pi}{2^{l-1}}x} = e^{i\pi x_{l-1}} e^{i\frac{\pi}{2}x_{l-2}} ... e^{i\frac{\pi}{2^{l-1}}x_0}.$$

Ici le point est que les bits x_i avec $i \geq l$ ne contribuent pas. Remplacant cette expression dans la formule du lemme, on trouve la décomposition finale qui permet de construire un circuit:

$$QFT|x\rangle = \prod_{l=1}^{m} \left(\frac{|0\rangle + e^{i\pi x_{l-1}} e^{i\frac{\pi}{2}x_{l-2}} ... e^{i\frac{\pi}{2^{l-1}}x_0}|1\rangle}{\sqrt{2}} \right).$$

La figure 7.7 représente le circuit correspondant à cette dernière formule pour $m = 4$, c.a.d $M = 16$. On peut se convaincre que l'opération de $SWAP$ requiert $O(3m)$ portes $CNOT$. D'autre part, le nombre de portes H et déphasages controlés est

$$m + (m-1) + ... + 1 = \frac{m(m+1)}{2}.$$

La profondeur du circuit est donc de l'ordre de $\mathrm{O}(m^2)$. Cette profondeur indique comment le temps de calcul pour la QFT augmente avec la taille des entrées.

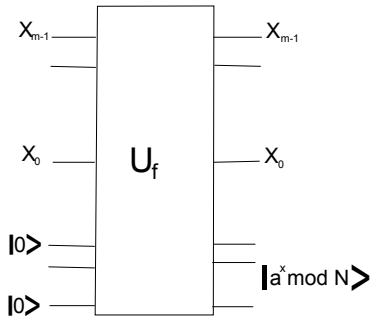


Figure 7.8 Représentation unitaire de l'exponentielle modulaire

D'autre part la largeur du circuit est m. Ainsi la taille totale est profondeur $\times$ largeur $= O(m^3)$.

7.7 Circuit pour $U_{f_{a,N}}$

Dans le chapitre précédent nous avons donné un algorithme aléatoire de factorisation d'entiers N basé sur la recherche de la période de l'exponentielle modulaire. Plus précisement, pour a t.q. PGCD$a, N = 1$, on cherche la période de la fonction $f_{a,N}(x) = a^x \mod N$. Ceci est équivalent à la recherche de $Ord_N(a) = r$ c.à.d le plus petit entier r t.q $a^r = 1 \mod N$.

Nous devons trouver un circuit qui réalise l'opérateur unitaire correspondant $U_{f_{a,N}}$. Notons d'abord que

$$\begin{aligned} a^x &= a^{2^{m-1}x_{m-1}} a^{2^{m-2}x_{m-2}} .... a^{2x_1} a^{x_0} \\ &= \left(a^{2^{m-1}}\right)^{x_{m-1}} \left(a^{2^{m-2}}\right)^{x_{m-2}} ... \left(a^2\right)^{x_1} a^{x_0}. \end{aligned}$$

Il est possible de pré-calculer les puissances $\{a, a^2, a^4, a^8, ..., a^{2^{m-1}}\}$ en un nombre polynomial d'opérations. En effet on part de a qui posséde m bits (au plus). Son carré a^2 se calcule en m^2 opérations. Puisque a^2 est pris $\mod M$, a^2 possède aussi m bits au plus. Le carré de ce dernier $a^4 = (a^2)^2$ se calcule en m^2 opérations, et ainsi de suite. En itérant ce procédé m fois, on va jusqu'au calcul de $a^{2^{m-1}}$. Ainsi on peut pré-calculer toutes ces puissances en $O(m^3)$ opérations. Il existe des circuits classiques réversibles pour faire ce calcul, et puisqu'ils sont réversibles, ils peuvent aussi être rendus quantiques (c.à.d unitaires). Finalement pour calculer a^x, en vertu de l'identité ci-dessus il suffit de prendre le circuit (figure 7.9): La profondeur de ce circuit est $O(m^3)$, sa largeur $O(m)$ et sa taille $O(m^4)$.

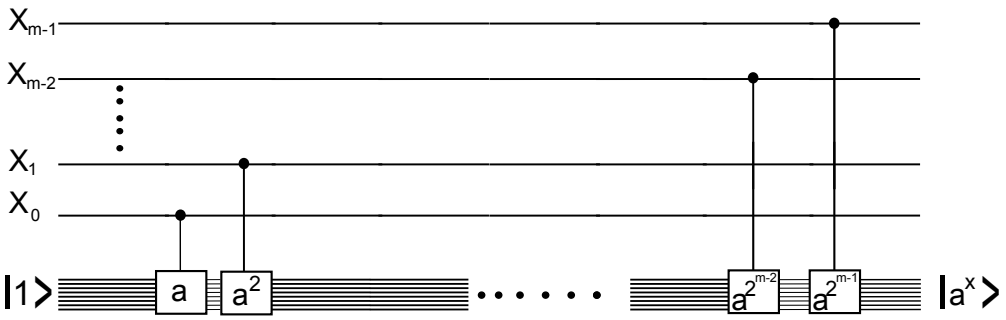


Figure 7.9 Circuit pour l'exponentielle modulaire.

7.8 Résumé de l'algorithme de Shor

Nous sommes maintenant en mesure de résumer la totalité de l'algorithme quantique de Shor pour la factorisation d'un entier N.

input: N impair et avec au moins deux facteurs premiers distincts.

output: facteur non trivial de N.

temps de calcul: $O((\ln N)^3 \ln\ln N |\ln \epsilon|)$ pour une probabilité de succès supérieure à $1-\epsilon$.

taille du circuit: $O((\ln N)^3)$.

Algorithme:

1. Choisir uniformément aléatoirement $a \in \{2....N-1\}$.
2. Calculer PGCD$a, N = d$ par l'algorithme d'Euclide:

- si $d > 1 \rightarrow$ SUCCES; on a un facteur,
- sinon $d = 1 \rightarrow$ aller en 3.

3. Calculer $Ord_N(a)$ (i.e $a^r = 1 \mod N$, trouver le plus petit r). Pour cela utiliser le circuit quantique avec m qubits et $2^m = M \approx N^2$. Faire une mesure quantique et considérer le résultat y. Calculer les convergents de $\frac{y}{M}$ (grâce à l'algorithme d'Euclide). Trouver si r se trouve parmi les dénominateurs de ces convergents en testant $a^r = 1 \mod N$.
- si oui (la théorie assure que c'est le plus petit possible) $\rightarrow$ aller en 4,
- sinon $\rightarrow$ ECHEC.

4. Verifier si r est pair et $a^r \neq -1 \mod N$
- si oui $\rightarrow$ aller en 5,
- sinon $\rightarrow$ ECHEC.

5. Calculer PGCD$a^{\frac{r}{2}}+1, N$ et PGCD$a^{\frac{r}{2}}-1, N$. Cela donne deux facteurs non triviaux de N (grâce à l'algorithme d'Euclide).

La probabilité de succès d'un tel "round" est $O\left(\frac{1}{\ln \ln N}\right)$ et sa complexité (temps de calcul) $O((\ln N)^3)$. On peut amplifier (comme d'habitude) la probabilité de succès à $1-\epsilon$ en faisant $O(\ln \ln N)$ rounds. Le temps de calcul total sera alors $O(|\ln \epsilon|(\ln \ln N)(\ln N)^3)$.

Part III

III. Réalisations Expérimentales

8 La Dynamique du Spin

Dans ce chapitre nous allons étudier la dynmique du spin 1/2 (moment magnétique de certains noyaux atomiques notamment). Celui-ci constitue l'une des réalisations naturelles les plus importantes du bit quantique. En effet celui-ci est aisément manipulable grâce à des champs magnétiques dépendant du temps. La manipulation et le contrôle des moments magnétiques par des champs magnétiques dépendant du temps est à la base de la Résonance Magnétique Nucléaire (utilisée pour l'imagerie IRM etc...). Ce contrôle des spins est aussi à la base de la réalisation des portes quantiques. Nous verrons dans ce chapitre comment réaliser les portes de Hadamard et NOT. Pour ce qui concerne la porte importante CNOT il faut d'abord comprendre comment interagissent les paires de moments magnétiques. Ce sera l'objet du chapitre 9.

8.1 La sphère de Bloch

Nous commençons par un petit rappel sur la sphère de Bloch déjà introduite au début du cours. Un qubit appartenant à l'espace d'Hilbert $\mathbb{C}^2$ peut toujours être paramétré comme suit

$$|\psi\rangle = (\cos\frac{\theta}{2})|\uparrow\rangle + (\sin\frac{\theta}{2})e^{i\phi}|\downarrow\rangle \tag{8.1}$$

Ce vecteur complexe à deux composantes, peut être représenté sur une sphère, appelée sphère de Bloch, où θ est l'angle par rapport à la direction z et ϕ est l'angle dans le plan xy par rapport à x.

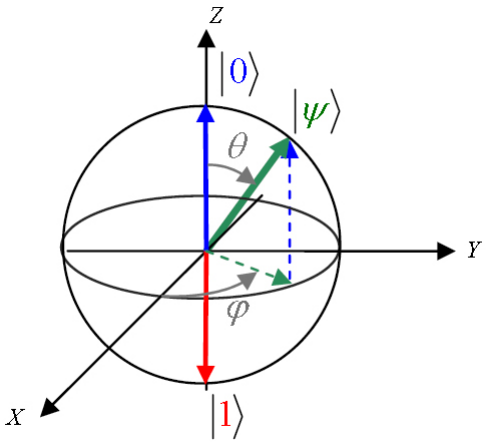


Figure 8.1 Sphère de Bloch

Il est utile de se remémorer (voir chapitre 2) la représentation des bases X, Y et Z c.à.d. $\{|+\rangle, |-\rangle\}$, $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$ et $\{|\uparrow\rangle, |\downarrow\rangle\}$ sur cette sphère. La base Z consiste en deux vecteurs opposés le long de l'axe z, la base X de deux vecteurs opposés le long de l'axe x et la base Y de deux vecteurs opposés le long de y.

Considérons la matrice

$$\vec{\sigma} \cdot \vec{n} = \sigma_x n_x + \sigma_y n_y + \sigma_z n_z \tag{8.2}$$

où $(\sigma_x, \sigma_y, \sigma_z)$ sont les trois matrices de Pauli et (n_x, n_y, n_z) est un vecteur unité tel que $n_x^2 + n_y^2 + n_z^2 = 1$. Soit aussi $n_x = \sin\theta\cos\phi$, $n_y = \sin\theta\sin\phi$ et $n_z = \cos\theta$. C'est à dire que $\vec{n}$ est "identique" à la représentation de $|\psi\rangle$ sur la sphère de Bloch. On peut vérifier que

$$\vec{\sigma} \cdot \vec{n}|\psi\rangle = (+1)|\psi\rangle \tag{8.3}$$

C'est à dire que $|\psi\rangle$ est un vecteur propre de $\vec{\sigma} \cdot \vec{n}$ avec valeur propre $+1$. On peut donc se faire l'image que "$|\psi\rangle$ sur la sphère de Bloch est la projection du vecteur $\vec{\sigma}$ sur l'axe $\vec{n}$".

Nous rappelons aussi la formule (analogue à la formule d'Euler) démontrée aux exercices

$$\exp(i\frac{\alpha}{2}\vec{\sigma} \cdot \vec{n}) = (\cos\frac{\alpha}{2})\mathbb{I} + i(\vec{\sigma} \cdot \vec{n})(\sin\frac{\alpha}{2}). \tag{8.4}$$

Pour comprendre la signification de cette matrice 2x2 considérons un cas particulier. Prenons $\vec{n} = (0, 0, 1)$ (c'.à.d. l'axe z) et appliquons la matrice sur $|\psi\rangle$.

$$\exp(i\frac{\alpha}{2}\sigma_z) = \exp(i\frac{\alpha}{2}\sigma_z)\left\{\cos\frac{\theta}{2}|\uparrow\rangle + e^{i\phi}\sin\frac{\theta}{2}|\downarrow\rangle\right\} \tag{8.5}$$

$$= e^{i\frac{\alpha}{2}}\cos\frac{\theta}{2}|\uparrow\rangle + e^{i\phi}e^{-i\frac{\alpha}{2}}\sin\frac{\theta}{2}|\downarrow\rangle \tag{8.6}$$

$$= e^{i\frac{\alpha}{2}}\left\{\cos\frac{\theta}{2}|\uparrow\rangle + e^{i(\phi-\alpha)}\sin\frac{\theta}{2}|\downarrow\rangle\right\} \tag{8.7}$$

Le préfacteur $e^{i\frac{\alpha}{2}}$ n'a pas de signification physique puisque c'est une phase globale. Le nouveau vecteur sur la sphère de Bloch fait toujours un angle θ avec z et un angle $(\phi - \alpha)$ dans le plan xy avec l'axe x. Ainsi l'opérateur $\exp(i\frac{\alpha}{2}\sigma_z)$ représente une rotation d'angle $(-\alpha)$ autour de l'axe z. De même la matrice $\exp(-i\frac{\alpha}{2}\sigma_z)$ représente une rotation d'angle $(+\alpha)$ autour de l'axe z.

Plus généralement la matrice $\exp(-i\frac{\alpha}{2}\vec{\sigma}\cdot\vec{n})$ représente une rotation d'angle $(+\alpha)$ et d'axe $\vec{n}$ sur la sphère de Bloch.

Nous allons voir que la dynamique du spin dans un champ $\vec{B}$ constant fait intervenir de telles relations (autour de $\vec{B}$ qui joue le rôle de $\vec{n}$ essentiellement).

8.2 L'Hamiltonien du spin dans un champ magnétique

Nous avons vu au début du cours que l'énergie d'interaction d'un moment magnétique $\vec{M}$ avec un champ magnétique $\vec{B}$ est donnée par (comme en physique classique):

$$E = -\vec{M}\cdot\vec{B} \tag{8.8}$$

En physique quantique l'observable $\vec{M}$ devient une matrice. Pour les moments magnétiques de spin 1/2 (comme celui de l'électron, du proton, de certains noyaux atomiques, etc..) on a

$$\vec{M} = \frac{g\hbar}{2}\vec{\sigma} \tag{8.9}$$

où $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ est le vecteur dont les composantes sont constituées par les trois matrices de Pauli. Ainsi l'énergie d'interaction d'un spin 1/2 dans un champ magnétique est donné par une matrice 2x2 (hermitienne car c'est une observable) appelée Hamiltonien

$$H = -\frac{g\hbar}{2}\vec{B}\cdot\vec{\sigma} \tag{8.10}$$

En composantes, cette matrice est explicitement

$$H = -\frac{g\hbar}{2}\begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix} \tag{8.11}$$

Considérons maintenant un champ magnétique constant (qui ne varie pas avec le temps). On peut toujours choisir l'axe z le long du vecteur $\vec{B} = (0, 0, B)$. Par conséquent:

$$H = -\frac{g\hbar}{2}B\sigma_z \equiv -\frac{\hbar\omega_0}{2}\sigma_z = -\frac{\hbar\omega_0}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{8.12}$$

où $\hbar\omega_0 = g\hbar B$ par définition. Ici ω_0 à l'unité d'une fréquence [s^{-1}] et s'appelle la fréquence de Larmor. Les deux valeurs propres de H sont $-\frac{\hbar\omega_0}{2}$ et $+\frac{\hbar\omega_0}{2}$ et les vecteurs propres correspondants sont $|\uparrow\rangle$ et $|\downarrow\rangle$. On peut représenter ces valeurs propres sur un diagramme donnant les "niveaux d'énergie" du système.

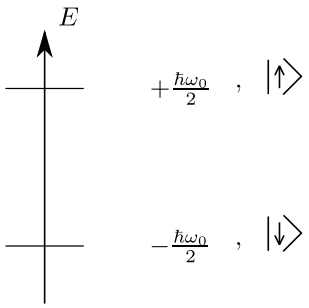


Figure 8.2 Niveaux d'énergie du système

Les systèmes dont l'Hamiltonien possède un spectre d'énergie de ce type s'appellent des "systèmes à deux niveaux". Il existe plusieurs types de systèmes à deux niveaux (exacts ou approximatifs) dans la nature. Ils peuvent tous être mathématiquement modélisés par "l'Hamiltonien d'un spin dans un champ magnétique", et donc le formalisme décrit dans ce chapitre dépasse de loin le cadre de la dynamique des moments magnétiques dans un champ magnétique.

Nous allons considérer aussi des champs magnétiques variables dans le temps du type

$$\vec{B} = (0, 0, B_0) + (B_1 \cos\omega t, B_1 \sin\omega t, 0) \tag{8.13}$$

Il s'agit d'un champ auquel on a ajouté une partie tournante dans le plan xy. L'Hamiltonien du spin dans ce champ est donné par la matrice

$$H = -\frac{g\hbar}{2}\begin{pmatrix} B_0 & B_1(\cos\omega t - \sin\omega t) \\ B_1(\cos\omega t + \sin\omega t) & B_0 \end{pmatrix} \tag{8.14}$$

En introduisant les matrices

$$\sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \text{et} \qquad \sigma_- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{8.15}$$

On peut réécrire cet Hamiltonien sous la forme

$$H = -\frac{\hbar\omega_0}{2}\sigma_z - \frac{\hbar\omega_1}{2}\left(\sigma_+ e^{-i\omega t} + \sigma_- e^{+i\omega t}\right) \tag{8.16}$$

Notons que $|\uparrow\rangle$ et $|\downarrow\rangle$ ne sont plus des états propres à cause du terme dépendant du temps. En fait ce terme est responsable de transitions quantiques entre ces états car

$$\sigma_+|\downarrow\rangle = |\uparrow\rangle \quad \text{et} \quad \sigma_+|\uparrow\rangle = 0 \tag{8.17}$$

$$\sigma_-|\uparrow\rangle = |\downarrow\rangle \quad \text{et} \quad \sigma_-|\downarrow\rangle = 0 \tag{8.18}$$

Nous allons voir que ces transitions entre les niveaux d'énergie de la partie $-\frac{\hbar\omega_0}{2}\sigma_z$ sont exploitées dans la RMN et la réalisation des portes logiques.

8.3 La précession de Larmor

Dans ce paragraphe nous étudions l'évolution temporelle d'un état $|\psi\rangle = (\cos\frac{\theta}{2})|\uparrow\rangle + e^{i\phi}(\sin\frac{\theta}{2})|\downarrow\rangle$ dans un champ magnétique constant $\vec{B} = (0, 0, B_0)$ orienté dans la direction z.

D'après les postulats de la mécanique quantique cette évolution temporelle est donnée par une matrice unitaire qui dépend du temps

$$U(t, 0)|\psi\rangle \equiv |\psi(t)\rangle \tag{8.19}$$

telle que $U(t_3, t_2)U(t_2, t_1) = U(t_3, t_1)$. (Ici $U(t, s)$ signifie l'évolution de l'instant s à l'instant t). Cette matrice est la solution de l'équation de Schrödinger:

$$i\hbar\frac{d}{dt}U(t, 0) = HU(t, 0) \tag{8.20}$$

Il s'agit donc de résoudre cette équation de Schrödinger.

La résolution est aisée si H ne dépend pas du temps t. En effet il est facile de vérifier qu'alors

$$U(t,0) = \exp(-i\frac{t}{\hbar}H) \tag{8.21}$$

est solution. Par contre si H dépend du temps la solution est plus compliquée et en particulier cette formule simple n'est plus valable.

Pour le cas du champ $\vec{B} = (0,0,B_0)$ constant où $H = -\frac{\hbar\omega_0}{2}\sigma_z$ indépendant du temps et donc:

$$U(t,0) = \exp(it\frac{\omega_0}{2}\sigma_z) \tag{8.22}$$

Nous reconnaissons ici la matrice de rotation autour de l'axe z et d'angle $(-t\omega_0)$. Ainsi l'état à l'instant t est

$$|\psi(t)\rangle = \exp\left(i\frac{t\omega_0}{2}\sigma_z\right)|\psi(0)\rangle \tag{8.23}$$

$$= \exp\left(i\frac{t\omega_0}{2}\sigma_z\right)\left\{\cos\frac{\theta}{2}|\uparrow\rangle + e^{i\phi}\sin\frac{\theta}{2}|\downarrow\rangle\right\} \tag{8.24}$$

$$= \exp\left(i\frac{t\omega_0}{2}\right)\cos\frac{\theta}{2}|\uparrow\rangle + e^{i\phi}\exp\left(-i\frac{t\omega_0}{2}\right)\sin\frac{\theta}{2}|\downarrow\rangle \tag{8.25}$$

$$= \exp\left(i\frac{t\omega_0}{2}\right)\left\{\cos\frac{\theta}{2}|\uparrow\rangle + \exp\left(i(\phi - t\omega_0)\right)\sin\frac{\theta}{2}|\downarrow\rangle\right\} \tag{8.26}$$

L'angle ϕ évolue comme $\phi - t\omega_0$ avec le temps. Sur la sphère de Bloch on a un mouvement appelé précession de Larmor autour de z (l'axe de $\vec{B}$) et la fréquence de la précession de Larmor est ω_0 lui-même (la périodicité temporelle étant $\frac{2\pi}{\omega_0} = T_0$).

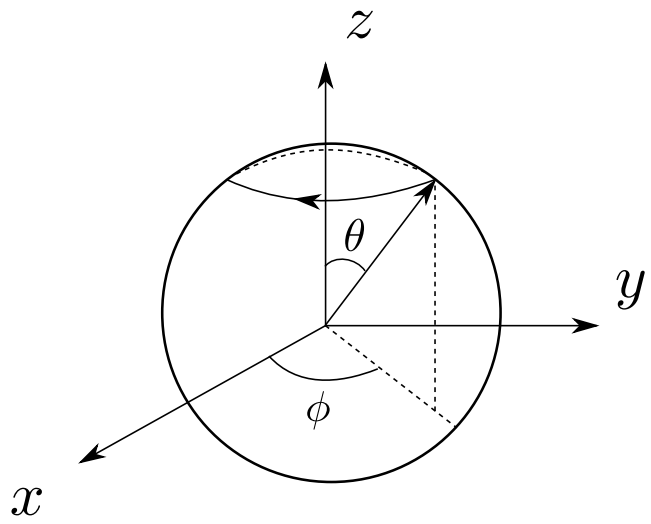


Figure 8.3 Précession de Larmor sur la sphère de Bloch

8.4 Oscillations de Rabi

Nous allons maintenant nous attaquer à la dynamique du spin dans le champs $\vec{B} = (0, 0, B_0) + B_1(\cos\omega t, \sin\omega t, 0)$ tournant.

L'équation de Schrödinger donnant l'opérateur d'évolution

$$i\hbar\frac{d}{dt}U(t,0) = H(t)U(t,0) \tag{8.27}$$

est toujours valable avec ici avec

$$H(t) = -\frac{\hbar\omega_0}{2}\sigma_z - \frac{\hbar\omega_1}{2}\left(\sigma_+ e^{-i\omega t} + \sigma_- e^{i\omega t}\right) \tag{8.28}$$

Néanmoins l'équation de Schrödinger est moins aisée à résoudre car H(t) dépend du temps. Pour nous affranchir de cette difficulté nous faisons un changement de référentiel. Dans le nouveau référentiel l'Hamiltonien est indépendant du temps et il est facile de calculer l'opérateur d'évolution. Soit:

$$|\tilde{\psi}(t)\rangle = \exp\left(i\frac{t}{\hbar}K\right)|\psi(t)\rangle \tag{8.29}$$

avec $K = \begin{pmatrix} -\frac{\hbar\omega}{2} & 0 \\ 0 & \frac{\hbar\omega}{2} \end{pmatrix}$.
Ici l'exponentielle est la matrice de rotation d'angle $(t\omega)$ autour de z. Puisque $|\psi(t)\rangle = U(t,0)|\psi(0)\rangle$ on trouve

$$|\tilde{\psi}(t)\rangle = \exp\left(i\frac{t}{\hbar}K\right)U(t,0)|\psi(0)\rangle \tag{8.30}$$

$$\equiv \tilde{U}(t,0)|\psi(0)\rangle \tag{8.31}$$

Ainsi le nouvel opérateur d'évolution dans le nouveau référentiel est $\tilde{U}(t,0) = e^{i\frac{t}{\hbar}K}U(t,0)$. Pour obtenir l'équation de Schrödinger on calcule:

$$i\hbar\frac{d}{dt}\tilde{U} = i\hbar\frac{i}{\hbar}Ke^{i\frac{t}{\hbar}K}U + e^{i\frac{t}{\hbar}K}H(t)U \tag{8.32}$$

$$= \left\{-K + e^{i\frac{tK}{\hbar}}H(t)e^{-i\frac{tK}{\hbar}}\right\}\tilde{U} \tag{8.33}$$

$$\equiv \tilde{H}(t)\tilde{U} \tag{8.34}$$

Le nouvel Hamiltonien est $\tilde{H}$. On le calcule facilement. En effet:

$$e^{i\frac{tK}{\hbar}} = \begin{pmatrix} e^{-i\frac{t\omega}{2}} & 0 \\ 0 & e^{i\frac{t\omega}{2}} \end{pmatrix} \tag{8.35}$$

ce qui donne finalement,

$$\tilde{H} = \frac{\hbar\delta}{2}\sigma_z - \frac{\hbar\omega_1}{2}\sigma_x \tag{8.36}$$

avec$\delta = \omega - \omega_0$. L'opérateur d'évolution $\tilde{U}$ est donc

$$\tilde{U} = \exp\left(-\frac{it}{\hbar}\tilde{H}\right) = \exp\left\{i\frac{t}{2}(\delta\sigma_z - \omega_1\sigma_x)\right\} \tag{8.37}$$

On peut calculer cette matrice à partir de la formule "d'Euler généralisée". A partir de là on déduit

$$U = e^{-i\frac{t}{\hbar}K}\tilde{U} \tag{8.38}$$

L'opérateur d'évolution final obtenu sans aucune approximation est:

$$U(t,0) = \begin{pmatrix} u_{\uparrow\uparrow} & u_{\uparrow\downarrow} \\ u_{\downarrow\uparrow} & u_{\downarrow\downarrow} \end{pmatrix} \tag{8.39}$$

avec les 4 éléments de matrice:

$$u_{\uparrow\uparrow} = e^{i\frac{t\omega}{2}}\left\{\cos\frac{t}{2}\sqrt{\delta^2+\omega_1^2} + i\frac{\delta}{\sqrt{\delta^2+\omega_1^2}}\sin\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right\} \tag{8.40}$$

$$u_{\uparrow\downarrow} = -i\frac{i\omega_1}{\sqrt{\delta^2+\omega_1^2}}e^{i\frac{t\omega}{2}}\sin\frac{t}{2}\sqrt{\delta^2+\omega_1^2} \tag{8.41}$$

$$u_{\downarrow\uparrow} = -i\frac{i\omega_1}{\sqrt{\delta^2+\omega_1^2}}e^{-i\frac{t\omega}{2}}\sin\frac{t}{2}\sqrt{\delta^2+\omega_1^2} \tag{8.42}$$

$$u_{\downarrow\downarrow} = e^{-i\frac{t\omega}{2}}\left\{\cos\frac{t}{2}\sqrt{\delta^2+\omega_1^2} - i\frac{\delta}{\sqrt{\delta^2+\omega_1^2}}\sin\frac{t}{2}\sqrt{\delta^2+\omega_1^2}\right\} \tag{8.43}$$

Nous avons complètement résolu le problème de la dynamique du vecteur d'état $|\psi\rangle$ dans un champs magnétique du type $(B_1\cos\omega t, B_1\sin\omega t, B_0)$. A partir de l'opérateur d'évolution on peut calculer les probabilité de transitions suivantes

$$P_{|\uparrow\rangle\to|\downarrow\rangle}(t) = |\langle\downarrow|U(t)|\uparrow\rangle|^2 = |u_{\uparrow\downarrow}|^2 \tag{8.44}$$

$$P_{|\uparrow\rangle\to|\uparrow\rangle}(t) = |\langle\uparrow|U(t)|\uparrow\rangle|^2 = |u_{\uparrow\uparrow}|^2 \tag{8.45}$$

La première probabilité représente la probabilité d'observer l'état $|\downarrow\rangle$ à l'instant t lorsque l'état initial est $|\uparrow\rangle$. C'est donc la probabilité que le spin soit "retourné". La seconde est la probabilité que le spin reste inchangé. On trouve:

$$\begin{cases} P_{|\uparrow\rangle\to|\downarrow\rangle}(t) &= \dfrac{\omega_1^2}{\delta^2+\omega_1^2}\left(\sin(\dfrac{t}{2}\sqrt{\delta^2+\omega_1^2})\right)^2 \\ P_{|\uparrow\rangle\to|\uparrow\rangle}(t) &= \left(\cos(\dfrac{t}{2}\sqrt{\delta^2+\omega_1^2})\right)^2 + \dfrac{\delta^2}{\delta^2+\omega_1^2}\left(\sin(\dfrac{t}{2}\sqrt{\delta^2+\omega_1^2})\right)^2 \end{cases} \tag{8.46}$$

On vérifie bien que ces deux probabilités se somment à 1, comme il se doit.

Le graphe suivant représente la probabilité de transition $P_{|\uparrow\rangle\to|\downarrow\rangle}(t)$ en fonction du temps. C'est une fonction périodique de période $T_{Rabi} = \frac{2\pi}{\sqrt{\delta^2+\omega_1^2}}$ et de hauteur $\frac{\omega_1^2}{\sqrt{\delta^2+\omega_1^2}}$. Nous voyons que l'amplitude est maximale lorsque $\delta = 0$ c.à.d. $\omega = \omega_0$, lorsque la fréquence du champs tournant est égale à la fréquence de Larmor. Lorsque $\delta \gg \omega_1$ (on parle de detuning) la probabilité de transition est faible.

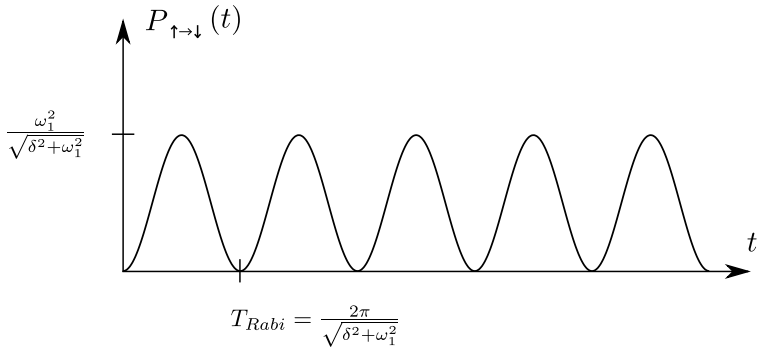


Figure 8.4 Probabilité de transition en fonction du temps

8.5 Réalisations des portes quantiques

Les oscillations de Rabi, appliquées au cas $\delta = 0$ ($\omega = \omega_0$ tuning parfait entre la fréquence de rotation du champ tournant et la fréquence de Larmor) permettent de réaliser certaines portes à 1 qubit. Ici nous discutons les portes NOT et de Hadamard.

*

La porte NOT

En prenant $\delta = 0$ et $t = \frac{T_{Rabi}}{2} = \frac{\pi}{\omega_1}$ on voit que $P_{|\uparrow\rangle\to|\downarrow\rangle} = 1$. Ainsi le spin est retourné avec probabilité 1 par un champ tournant tel que $\omega = \omega_0$ enclenché pendant un temps $t = \frac{\pi}{\omega_1}$. Un tel champ s'appelle un "π-pulse" dans le language de la RMN. Le temps $t = \frac{\pi}{\omega_1}$ est en gros la durée de basculement du spin.

Pour vérifier que l'opérateur d'évolution unitaire correspond bien (est équivalent) à la porte NOT, il est commode d'examiner l'évolution dans le référentiel tournant

$$\tilde{U} = \exp\left(i\frac{t}{2}(\delta\sigma_z + \omega_1\sigma_x)\right). \tag{8.47}$$

Pour $\delta = 0$ et $t = \frac{\pi}{\omega_1}$ on trouve

$$\tilde{U} = \exp(i\frac{\pi}{2}\sigma_x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{8.48}$$

Il s'agit d'une matrice de rotation d'angle π autour de l'axe x. Le vecteur $|\uparrow\rangle$ est bien transformé en $|\downarrow\rangle$ et $|\downarrow\rangle$ est bien transformé en $|\uparrow\rangle$.

*

La porte de Hadamard

Cette fois on fixe $\delta = 0$ (tuning parfait $\omega = \omega_0$) et on enclenche le champ tournant $(B_1 \cos\omega t, B_1 \sin\omega t, B_0)$ pendant un temps $t = \frac{T_{Rabi}}{4} = \frac{\pi}{2\omega_1}$. Notez que cette durée est la moitié de celle de la porte NOT. On trouve alors $P_{|\uparrow\rangle\to|\downarrow\rangle} = \frac{1}{2}$ et $P_{|\downarrow\rangle\to|\uparrow\rangle} = \frac{1}{2}$. Plus précisément dans le référentiel tournant

$$\tilde{U} = \exp\left(i\frac{t}{2}(\delta\sigma_z + \omega_1\sigma_x)\right) \tag{8.49}$$

$$= \exp\left(i\frac{\pi}{4}\sigma_x\right) \tag{8.50}$$

$$= \left(\cos\frac{\pi}{4}\right)\mathbb{I} + i\left(\sin\frac{\pi}{4}\right)\sigma_x \tag{8.51}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix} \tag{8.52}$$

Cette matrice effectue le basculement de $|\uparrow\rangle$ vers $\frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\downarrow\rangle)$ et le basculement de $|\downarrow\rangle$ vers $\frac{1}{\sqrt{2}}(i|\uparrow\rangle + |\downarrow\rangle) = \frac{i}{\sqrt{2}}(|\uparrow\rangle - i|\downarrow\rangle)$. Cette opération est physiquement équivalente à une porte de Hadamard, $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$.

9 Hamiltonien de Heisenberg et Portes à deux qubits

Dans le chapitre 8 nous avons discuté la dynamique du spin dans un champ magnétique dépendant du temps. Cela permet comme nous l'avons vu de réaliser des portes à 1 qubit. Par exemple nous avons vu comment réaliser les portes NOT et Hadamard. Pour implémenter le calcul quantique, il faut encore être capable de réaliser des portes à deux qubits. Nous avons vu que l'ensemble des portes universelles contient CNOT et en principe cette porte à 2 qubits suffit à fabriquer n'importe quel circuit. Cette porte fait intervenir 2 qubits et ne peut être réalisée qu'à partir de leur interaction. Cela est généralement vrai pour toute porte à 2 qubits (qui est non triviale). Pour cette raison nous allons tout d'abord étudier l'interaction entre deux moments magnétiques. Nous verrons ensuite qu'avec certaines formes de cette interaction magnétique il est possible de fabriquer les portes voulues. De telles interactions magnétiques abondent dans la nature. Ce point sera discuté au chapitre 10.

9.1 Hamiltonien d'Heisenberg

Nous avons vu que l'énergie d'interaction entre un moment magnétique $\vec{M}$ et un champ magnétique $\vec{B}$ est donné par $-\vec{B} \cdot \vec{M}$. Considérons maintenant deux moments magnétiques $\vec{M_1}$ et $\vec{M_2}$. On peut penser à ceux-ci comme à deux petits aimants. Pour minimiser leur énergie ceux-ci vont avoir tendance à s'éloigner de façon "antiparallèle" comme sur la figure:

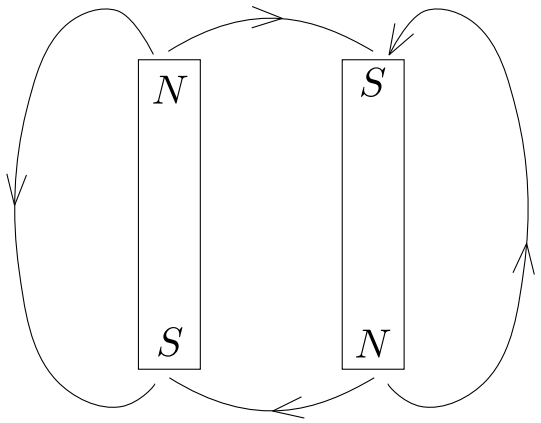


Figure 9.1 Lignes de champs de deux dipôles magnétiques

Ici les boucles représentent les lignes du champ magnétique. Si nous demandons que l'énergie d'interaction soit indépendante de l'orientation globale du système, c'est-à-dire qu'il n'y a pas de direction privilégiée; on peut prendre comme Hamiltonien simple (ici " $\approx$ proportionnel "):

$$H \approx \vec{M}_1 \cdot \vec{M}_2 \tag{9.1}$$

Notons aussi que cette expression est la seule possible qui soit à la fois invariante sous les rotations du référentiel (pas de direction privilégiée) et du premier ordre dans $\vec{M}_1$ et $\vec{M}_2$.

Pour les moments magnétiques quantiques intrinsèques de spin $1/2$ (par exemple proton, noyaux atomiques ^{13}C, ^{19}C, etc.) nous savons que $\vec{M}_1 = g_1 \frac{\hbar}{2} \vec{\sigma_1}$ et $\vec{M}_2 = g_2 \frac{\hbar}{2} \vec{\sigma_2}$ où $\vec{\sigma_1}$ et $\vec{\sigma_2}$ sont les vecteurs des matrices de Pauli et g_1, g_2 dépendent du type précis de noyaux. L'Hamiltonien d'interaction entre deux moments magnétiques quantiques de spin $1/2$ est donc donné par (sysème invariant de rotation):

$$H = \hbar J \vec{\sigma_1} \cdot \vec{\sigma_2} \tag{9.2}$$

où $\hbar J$ à l'unité d'énergie et J l'unité d'une fréquence $[\mathrm{s}^{-1}]$.

Faisons quelques remarques importantes sur l'interprétation du produit scalaire ci-dessus. Tout d'abord $\vec{\sigma_1} \cdot \vec{\sigma_2}$ doit être une matrice 4×4 puisqu'il s'agit d'une observable (matrice hermitienne) agissant sur les états de deux qubits (sur l'espace d'Hilbert $\mathbb{C}^2 \otimes \mathbb{C}^2$). Ainsi

$$\vec{\sigma_1} \cdot \vec{\sigma_2} = \sigma_1^x \otimes \sigma_2^x + \sigma_1^y \otimes \sigma_2^y + \sigma_1^z \otimes \sigma_2^z. \tag{9.3}$$

Explicitement, dans la base canonique

$$\sigma_1^x \otimes \sigma_2^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{9.4}$$

$$\sigma_1^y \otimes \sigma_2^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{9.5}$$

$$\sigma_1^z \otimes \sigma_2^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{9.6}$$

Et donc

$$H = \hbar J \vec{\sigma_1} \cdot \vec{\sigma_2} = \hbar J \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{9.7}$$

Il est facile de calculer les valeurs propres (niveaux d'énergie) et vecteurs propres de cette matrice. Néanmoins il est encore plus instructif de le faire en utilisant l'algèbre de Pauli.

Introduisons les matrices

$$\sigma^+ = \frac{1}{2}(\sigma^x + i\sigma^y) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{9.8}$$

$$\sigma^- = \frac{1}{2}(\sigma^x - i\sigma^y) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{9.9}$$

Le lecteur vérifiera que $\sigma^+|\uparrow\rangle = 0$, $\sigma^+|\downarrow\rangle = |\uparrow\rangle$, $\sigma^-|\downarrow\rangle = 0$, $\sigma^-|\uparrow\rangle = |\downarrow\rangle$. En exprimant σ^x et σ^y en fonction de σ^+ et σ^- il est facile de montrer que

$$H = \hbar J \Big\{ \sigma_1^z \otimes \sigma_2^z + 2\big(\sigma_1^+ \otimes \sigma_2^- + \sigma_1^- \otimes \sigma_2^+\big) \Big\} \tag{9.10}$$

On peut vérifier que les éléments de matrice $\langle s_1' s_2' | H | s_1 s_2 \rangle$ où s_1, s_2, s_1', $s_2' = \uparrow$, $\downarrow$ donnent la matrice écrite précédemment. Par exemple

$$H|\uparrow\downarrow\rangle = 2\hbar J(\sigma_1^- \otimes \sigma_2^+)|\uparrow\downarrow\rangle \tag{9.11}$$
$$= 2\hbar J|\downarrow\uparrow\rangle \tag{9.12}$$

Si bien que $\langle\downarrow\uparrow|H|\uparrow\downarrow\rangle = 2\hbar J$.

Considérons maintenant l'action de H sur l'état $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ (Notez que cet état est l'un des états de Bell).

$$\sigma_1^z \otimes \sigma_2^z(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{9.13}$$
$$\sigma_1^+ \otimes \sigma_2^-(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -|\uparrow\downarrow\rangle \tag{9.14}$$
$$\sigma_1^- \otimes \sigma_2^+(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = |\downarrow\uparrow\rangle. \tag{9.15}$$

Ces trois équations impliquent

$$H(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -3\hbar J(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle). \tag{9.16}$$

L'état $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ est donc un état propre de H d'énergie $-3\hbar J$.

Considérons l'action de H sur les trois états $|\uparrow\uparrow\rangle$; $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$ et $|\downarrow\downarrow\rangle$. On voit facilement que $(\sigma_1^+ \otimes \sigma_2^- + \sigma_1^- \otimes \sigma_2^+)$ s'annule contre ces trois états. Il reste donc l'action de $\sigma_1^z \otimes \sigma_2^z$ qui donne

$$H|\uparrow\uparrow\rangle = \hbar J|\uparrow\uparrow\rangle \tag{9.17}$$
$$H(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) = \hbar J(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{9.18}$$
$$H|\downarrow\downarrow\rangle = \hbar J|\downarrow\downarrow\rangle \tag{9.19}$$

Ainsi ces 3 états sont états propres de H avec niveaux d'énergie (valeur propre) $+\hbar J$.

En résumé l'état fondamental de H est l'état dit "singulet" d'énergie $-3\hbar J$ et les autres états dits "triplets" possédant tous la même énergie $+\hbar J$.

A titre d'exercice regardons l'effet d'un champ magnétique extérieur $\vec{B}$ sur les niveaux d'énergie du système. L'Hamiltonien devient:

$$H = -\frac{\hbar g_1}{2}\vec{B}\cdot\vec{\sigma_1} - \frac{\hbar g_2}{2}\vec{B}\cdot\vec{\sigma_2} + \hbar J\vec{\sigma_1}\cdot\vec{\sigma_2} \tag{9.20}$$

Notez que le terme $\vec{B}\cdot\vec{\sigma_1}$ doit être interprété comme $(\vec{B}\cdot\vec{\sigma_1}\otimes\mathbb{I}_2)$ et le terme $\vec{B}\cdot\vec{\sigma_2}$ doit être interprété comme $(\mathbb{I}_1 \otimes \vec{B}\cdot\vec{\sigma_2})$. Il est clair que nous pouvons orienté $\vec{B}$ le long de l'axe z. Puisque l'interaction magnétique $\hbar J\vec{\sigma_1}\cdot\vec{\sigma_2}$ est invariante sous les rotations cela ne fait pas de différence sur les niveaux d'énergie.

Considérons le cas le plus simple de deux noyaux identique $g_1 = g_2$. Alors en

posant aussi $\hbar g B = \hbar\omega_0$ (la fréquence de Larmor) on est amené à étudier les niveaux d'énergie de

$$H = -\frac{\hbar\omega_0}{2}\left(\sigma_1^z \otimes \mathbb{I}_2 + \mathbb{I}_1 \otimes \sigma_2^z\right) + \hbar J \vec{\sigma_1} \cdot \vec{\sigma_2} \tag{9.21}$$

On a

$$H|\uparrow\uparrow\rangle = (-\hbar\omega_0 + \hbar J)|\uparrow\uparrow\rangle \tag{9.22}$$
$$H|\downarrow\downarrow\rangle = (+\hbar\omega_0 + \hbar J)|\downarrow\downarrow\rangle \tag{9.23}$$
$$H(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) = \hbar J(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{9.24}$$
$$H(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -3\hbar J(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{9.25}$$

Nous voyons que l'énergie de l'état singulet est inchangée. Cela n'est pas surprenant puisque dans cet état les composantes z du spin sont opposées. La même remarque vaut pour l'état $(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$. Les états $|\uparrow\uparrow\rangle$ et $|\downarrow\downarrow\rangle$ voient leurs énergies descendre (orientation parallèle à $\vec{B}$) et monter (orientation anti-parallèle à $\vec{B}$). Le point important ici et que la dégénérescence de l'état triplet est "levée" par la perturbation additionnelle: ceci est une caractéristique assez générique en MQ. Le graphe de l'énergie des états en fonction de B ou ω_0 est donné ci-dessous:

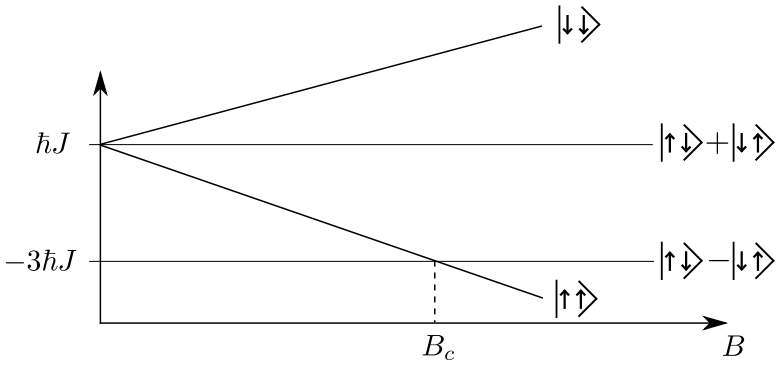


Figure 9.2 Graphe de l'énergie des états

Il existe un champ critique au-delà duquel c'est l'état $|\uparrow\uparrow\rangle$ qui devient état de plus basse énergie (état fondamental).

9.2 Porte SWAP et Hamiltonien de Heisenberg

La porte SWAP est donnée par la définition suivante sur les états de la base computationnelle:

$$SWAP|x,y\rangle = |y,x\rangle \tag{9.26}$$

Par linéarité cette définition s'étend sur tout l'espace de Hilbert. Cette porte est importante car elle permet d'échanger les qubits d'un circuit. De plus on peut réaliser une porte SWAP à partir de 3 portes CNOT comme suit:

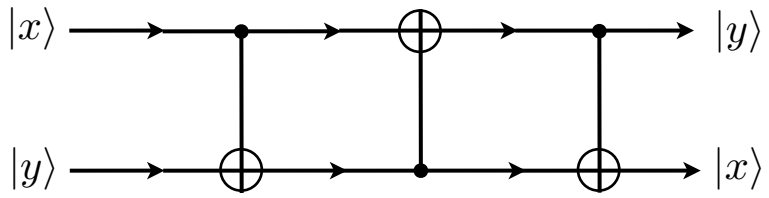


Figure 9.3 Circuit pour la réalisation du SWAP

De plus on peut montrer qu'il est possible de réaliser CNOT à partir de $\sqrt{SWAP}$ et de portes à 1 qubit. Ainsi $\sqrt{SWAP}$ joue aussi le rôle de porte universelle au même titre que CNOT.

Dans ce paragraphe nous montrons que SWAP peut être réalisée grâce à l'Hamiltonien de Heisenberg isotrope. De même $\sqrt{SWAP}$ peut aussi être fabriqué avec ce même Hamiltonien.

Calculons tout d'abord l'opérateur d'évolution pour l'Hamiltonien d'Heisenberg.

$$U_{Heis}(t) = \exp\left(-\frac{it}{\hbar}H_{Heis}\right). \tag{9.27}$$

Nous allons le faire en notation de Dirac et dans la base des états propres de cette Hamiltonien. Sa décomposition spectrale est:

$$H = -3\hbar J\left\{\frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}\cdot\frac{\langle\uparrow\downarrow| - \langle\downarrow\uparrow|}{\sqrt{2}}\right\} \tag{9.28}$$

$$+\hbar J\left\{|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}}\cdot\frac{\langle\uparrow\downarrow| + \langle\downarrow\uparrow|}{\sqrt{2}} + |\downarrow\downarrow\rangle\langle\downarrow\downarrow|\right\} \tag{9.29}$$

Dans la base des états propres il suffit de calculer l'exponentielle des valeurs propres:

$$U_{Heis}(t) = e^{i3Jt}\left\{\frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}\cdot\frac{\langle\uparrow\downarrow| - \langle\downarrow\uparrow|}{\sqrt{2}}\right\} \tag{9.30}$$

$$+e^{-itJ}\left\{|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}}\cdot\frac{\langle\uparrow\downarrow| + \langle\downarrow\uparrow|}{\sqrt{2}} + |\downarrow\downarrow\rangle\langle\downarrow\downarrow|\right\} \tag{9.31}$$

Un bon exercice que nous laissons au lecteur est d'écrire à partir de cette expression la matrice en composantes dans la base canonique $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle$.

Prenons maintenant $t = \frac{\pi}{4J}$. C'est à dire que nous supposons que l'interaction magnétique est enclenchée pendant un intervalle de temps $\frac{\pi}{4J}$ seulement. Bien sûr en pratique cela pose un problème car on ne peut pas enclencher et déclencher à volonté les interactions magnétiques entre moments magnétiques. Mais nous verrons au chapitre suivant comment "la technique de refocalisation" permet de remédier à ce problème.

Pour $t = \frac{\pi}{4J}$ on a $e^{i3Jt} = e^{i\frac{3\pi}{4}} = -e^{i\frac{\pi}{4}}$ et $e^{-tiJ} = e^{-i\frac{\pi}{4}}$. Ainsi

$$U_{Heis}(\frac{\pi}{4J}) = e^{-i\frac{\pi}{4}}\Big\{-\frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| - \langle\downarrow\uparrow|}{\sqrt{2}} \tag{9.32}$$

$$+ |\uparrow\uparrow\rangle\langle\uparrow\uparrow| + \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}} \cdot \frac{\langle\uparrow\downarrow| + \langle\downarrow\uparrow|}{\sqrt{2}} + |\downarrow\downarrow\rangle\langle\downarrow\downarrow|\Big\} \tag{9.33}$$

Il est facile de voir sur cette formule que

$$U_{Heis}(\frac{\pi}{4J})|\uparrow\uparrow\rangle = e^{-i\frac{\pi}{4}}|\uparrow\uparrow\rangle \tag{9.34}$$

$$U_{Heis}(\frac{\pi}{4J})|\downarrow\downarrow\rangle = e^{-i\frac{\pi}{4}}|\downarrow\downarrow\rangle \tag{9.35}$$

$$U_{Heis}(\frac{\pi}{4J})(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) = e^{-i\frac{\pi}{4}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{9.36}$$

$$U_{Heis}(\frac{\pi}{4J})(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) = -e^{-i\frac{\pi}{4}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{9.37}$$

$$= e^{-i\frac{\pi}{4}}(|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle) \tag{9.38}$$

A une phase gloable près (qui n'est pas importante physiquement) nous voyons que $U_{Heis}(\frac{\pi}{4J})$ échange bien les deux qubits. Sous cet échange l'état triplet reste invariant et l'état singulet change de signe. Notez que l'addition et la soustraction des deux dernières équations donnent bien:

$$U_{Heis}(\frac{\pi}{4J})|\uparrow\downarrow\rangle = e^{-i\frac{\pi}{4}}|\downarrow\uparrow\rangle \tag{9.39}$$

$$U_{Heis}(\frac{\pi}{4J})|\downarrow\uparrow\rangle = e^{-i\frac{\pi}{4}}|\uparrow\downarrow\rangle \tag{9.40}$$

qui n'est rien d'autre que le SWAP.

Pour obtenir $\sqrt{SWAP}$ il suffit de choisir $t = \frac{\pi}{8j}$ au lieu de $\frac{\pi}{4J}$!

9.3 Porte CNOT et interaction magnétique anisotrope

Si les moments magnétiques sont dans un environnement anisotrope alors l'Hamiltonien de Heisenberg devient anisotrope lui aussi. Un cas extrême, mais qui est une très bonne approximation dans certaines expériences de RMN (voir chapitre sur les

réalisations expérimentales suivant) est celui d'une anisotropie où la direction z est dominante (par exemple à cause du champ externe $\vec{B_0} = (0, 0, B_0)$ très puissant par rapport aux interactions magnétiques). Dans ces cas un Hamiltonien qui décrit le sysème raisonnablement bien est

$$H = \hbar J \sigma_1^z \otimes \sigma_2^z. \tag{9.41}$$

Cet Hamiltonien est purement diagonal:

$$H = \hbar J \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \hbar J \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{9.42}$$

$$= \hbar J \Big\{ |\uparrow\uparrow\rangle\langle\uparrow\uparrow| - |\uparrow\downarrow\rangle\langle\uparrow\downarrow| - |\downarrow\uparrow\rangle\langle\downarrow\uparrow| + |\downarrow\downarrow\rangle\langle\downarrow\downarrow| \Big\} \tag{9.43}$$

L'opérateur d'évolution est donc

$$e^{-i\frac{t}{\hbar}H} = e^{-itJ}|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + e^{itJ}|\uparrow\downarrow\rangle\langle\uparrow\downarrow| + e^{itJ}|\downarrow\uparrow\rangle\langle\downarrow\uparrow| + e^{-itJ}|\downarrow\downarrow\rangle\langle\downarrow\downarrow| \tag{9.44}$$

$$= \begin{pmatrix} e^{-itJ} & 0 & 0 & 0 \\ 0 & e^{itJ} & 0 & 0 \\ 0 & 0 & e^{itJ} & 0 \\ 0 & 0 & 0 & e^{-itJ} \end{pmatrix} \tag{9.45}$$

Aux exercices vous avez démontré l'identité suivante:

$$CNOT = (\mathbb{I}_1 \otimes H_2)(R_1 \otimes R_2) e^{-\frac{i}{\hbar}\frac{\pi}{4J}H} (\mathbb{I}_1 \otimes H_2) \tag{9.46}$$

où $R_1 = \exp(-i\frac{\pi}{4}\sigma_1^z)$ et $R_2 = \exp(-i\frac{\pi}{4}\sigma_2^z) = \begin{pmatrix} e^{-i\frac{\pi}{4}} & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$.

Ainsi la porte CNOT peut être réalisée en "enclenchant" l'interaction magnétique pendant un temps $\frac{\pi}{4J}$ et en combinant cela avec des manipulations à 1 qubit. A nouveau, en pratique il faut utiliser la "technique de refocalisation" pour "enclencher" et "déclencher" l'interaction magnétique.

Le circuit associé à la réalisation de CNOT est le suivant (voir l'identité ci-dessus):

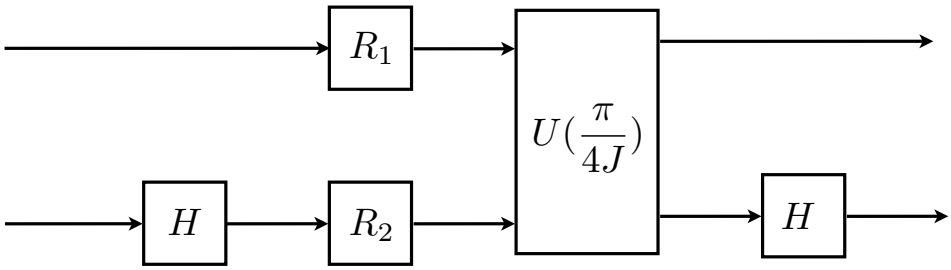


Figure 9.4 Circuit pour la réalisation du CNOT

10 Réalisations expérimentales

Nous exposons dans ce chapitre les principes de base des réalisations expérimentales des algorithmes quantiques. L'illustration des principes sera faite dans le cadre de la résonance magnétique nucléaire (RMN), qui comme nous le verrons, a permis de réaliser certains algorithmes, tels que celui de Shor, en laboratoire. Même s'il n'est probablement pas possible d'aller au delà d'une dizaine de qubits avec la RMN, celle-ci a l'avantage d'illustrer de facon concrète et simple les principes universels qui s'appliquent aussi bien à d'autres technologies plus prometteuses. En effet quelque soit la technologie sous-jacente pour la fabrication et la manipulation de qubits effectifs, les hamiltoniens régissant leur dynamique ne peuvent être que des "polynomes" exprimés à partir des matrices de Pauli, contenant des termes linéaires et quadratiques à l'ordre le plus bas.

10.1 Les systèmes en jeu

Dans le cas de la RMN les qubits sont les moments magnétiques de noyaux atomiques de spin 1/2, de molécules appropriées. Ces molécules sont naturelles ou éventuellement synthétiques, et forment un fluide ou solide macroscopique. La figure 10.1 montre deux molécules naturelles - le chloroforme et le trichloroétylène - qui ont déjà été utilisées pour le calcul quantique. Comme nous le verrons, chaque molécule correspond en quelque sorte à un circuit quantique. Dans ces molécules les qubits en jeu sont les spin 1/2 des noyaux d'hydrogène ^1H, de carbone ^{13}C et de fluor ^{19}F. Le noyau de l'atome hydrogène est un proton qui possède un spin 1/2. Le ^{13}C contient 6 protons et 7 neutrons[1]. Dans l'état fondamental du noyau les spins des protons et neutrons se compensent entre eux, si bien que le spin total est 1/2. La situation est similaire pour l'isotope ^{19}F du fluor qui possède 9 protons et 10 neutrons.

Le fluide (ou le solide) à température ambiante, est placé dans une région ou règne un champ magnétique statique $\vec{B}_0 = (0, 0, B_0)$ orienté dans la direction z, d'intensité $B_0 \approx 1 - 10\text{T}$. Il s'agit d'un champ très intense: $1\text{T} = 10^5$ Gauss, le

[1] Il s'agit de l'isotope du ^{12}C contenant 6 protons et 6 neutrons et possède un spin total nul; le ^{14}C connu pour être utilisé pour la datation, est un autre isotope contenant 6 protons et 8 neutrons, et son spin total est aussi nul. Les atomes de carbone sont électriquement neutres et contiennent tous 6 électrons; les propriétés chimiques sont régies par le nuage électronique et sont donc identiques pour des isotopes.

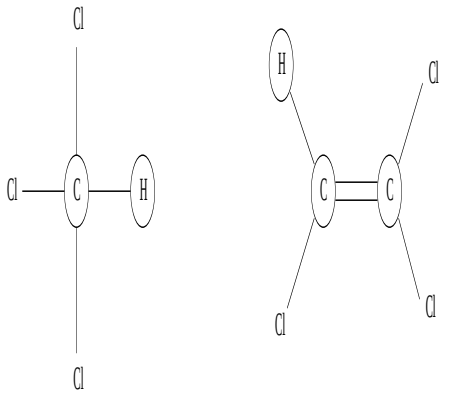


Figure 10.1 Molécules de chloroforme (gauche) et trichloroéthylène (droite). Les atomes d'hydrogène ^1H, carbone ^{13}C et fluor ^{19}F dont le noyau de spin 1/2 est un qubit, sont entoures. Les noyaux des atomes de chlore possèdent un spin nul et ne sont pas des qubits.

Gauss étant l'ordre de grandeur du champ magnétique terrestre. Les fréquences de Larmor des moments magnétiques des noyaux ^1H, ^{13}C, ^{19}F sont de l'ordre de grandeur $\omega_L \approx 10 - 100\text{MHz}$ ($1\text{MHz} = 10^6\text{Hz}$).

Les portes à un qubit sont réalisées par des pulses de radiofréquence $\vec{B}_1 e^{i\omega t}$ d'intensité $\omega_1 \approx 0.1 - 1\text{MHz}$. Ces pulses sont générés par une ou des bobines parcourues par un courant alternatif de radiofréquence ω. Il est possible d'agir sélectivement sur un type de qubit ^1H, ^{13}C, ^{19}F en réglant ω sur la fréquence de Larmor du qubit (cas résonant). L'influence sur les autres qubits ayant une fréquence de Larmor différente (non résonnante) peut être négligé. Nous verrons que l'environnement chimique d'un qubit dans la molécule a un effet correctif sur les fréquences de Larmor. Ce point est important, d'une part car il faut régler les fréquences de résonance suffisamment précisément, et d'autre part car cela permet d'agir sélectivement et distinguer les qubits de noyaux identiques. L'intensité ω_1 donne l'ordre de grandeur de la durée de la porte $\tau_1 \approx \frac{2\pi}{\omega_1} \approx 10^{-6}$ sec.

Les portes à deux qubit sont réalisées par la nature elle-même. Comme nous le verrons, il est possible de prendre avantage de l'interaction spin-spin de type Heisenberg pour réaliser des portes à deux qubits. La durée de ces portes est déterminée par l'intensité du couplage spin-spin, et est d'environ 10^{-3} sec. Celle-ci est donc mille fois plus longue que la durée des portes à un qubit. Cette dernière pourra en première approximation être négligée.

A ce point il est instructif de se faire une image des différentes échelles d'énergies en jeu. Le "circuit quantique moléculaire" est controllé grâce aux pulses de radiofréquence. L' énergie mise en jeu dans ces pulses de radio-fréquence est $\hbar\omega_1 \approx 10^{-6}$ eV. Celle-ci est au moins mille fois plus faible que toutes les autres énergies en jeu, si bien que ces pulses n'affectent en rien la structure moléculaire.

En effet les énergies d'excitations du nuage électronique sont de l'ordre de l'eV[2]; l'énergie du spitting Zeeman des spins électroniques est de l'ordre de 10^{-3} eV[3].

Le calcul quantique par RMN porte simultanément sur un nombre macroscopique de molécules, et la mesure collective finale produit directement un résultat statistique. Pour pouvoir manipuler les moments magnétiques des noyaux actifs dans la molécule il faut pouvoir caractériser et séparer de facon suffisamment précise leurs fréquences de Larmor. Ceci n'est possible que pour des molécules de tailles relativement, faibles contenant jusqu'à une dizaine de qubits. Même s'il était possible de synthétiser des molécules avec une centaine ou un millier de noyaux représentant les qubits actifs, les fréquences de Larmor formeraient un quasi-continuum et il deviendrait difficile de les manipuler et/ou de maintenir la cohérence des états quantiques. En effet dans ce cas, d'une part les énergies d'excitations thermiques, et d'autre part la largeur des pulses de radiofréquence sont plus grandes que les différences entre fréquences de Larmor. C'est une des raisons pour lesquelles il n'a pas été encore possible d'utiliser la RMN pour fabriquer un ordinateur quantique fonctionnant sur plus d'une dizaine de qubits. Une autre raison importante provient du fait que les spins de l'état initial ne sont pas suffisamment bien polarisés, et leur état est loin d'être un état pur. C'est un état équilibre thermique. Une des innovations des expériences par RMN fut de transformer l'état thermique en état "pseudo-pur". Ce dernier point dépasse le cadre de ce cours ne sera pas abordé ici[4].

10.2 Oscillations de Rabi et portes à un qubit

Ce paragraphe résume l'essentiel de la théorie des oscillations de Rabi, qui sont à la base de la réalisation des portes à un qubit telles que les portes de Hadamard, les rotations autour de x, y ou z, ou encore les $\pi/2^k$ shifts.

L'hamiltonien d'un moment magnétique dans un champ $\vec{B}_0 = (0, 0, B_0)$ est

$$H = -\frac{g\hbar}{2m}\vec{B}_0 \cdot \vec{\sigma} = -\frac{\hbar\omega_L}{2}\sigma_z.$$

Pour le noyau d'hydrogène ${}^1H$, $g \approx 5.59$, $m = 10^{-27}$ kg et $q = 1,6\,10^{-19}$ C, ce qui donne une fréquence de Larmor $\omega_L \approx 100$ MHz. L'évolution temporelle d'un état est donnée par[5]

$$|\psi\rangle = e^{i\frac{\varphi+\omega_L t}{2}} \cos\frac{\theta}{2}|\uparrow\rangle + e^{-i\frac{\varphi+\omega_L t}{2}} \sin\frac{\theta}{2}|\downarrow\rangle.$$

[2] 1 eV $= 1,6\,10^{-19}$ Joule, J $= \mathrm{kg\,m^2/s^2}$, et $\hbar = 6,58211928(15).10^{-16}$ eV.

[3] L'énergie d'excitation interne des noyaux est 10^6 eV, et pour les nucléons $\sim 10^9$ eV (l'échelle de la chromodynamique quantique).

[4] A titre d'information indiquons qu'un état pseudo-pur est une matrice densité de la forme $\rho = \alpha Id + \delta|\Psi\rangle\langle\Psi|$. La moyenne de toute observable A à trace nulle, satisfait $\mathrm{Tr}\rho A = \delta\langle\Psi|A|\Psi\rangle$. Lorsque l'on transforme l'état thermique en état pseudo-pur, δ diminue avec le nombre de qubits et le signal résultant de la mesure devient trop faible

[5] L'état initial est obtenu en posant $t = 0$.

On peut se faire une image de cette dynamique en représentant l'état par un vecteur sur la sphère de Bloch. Ce vecteur possède un angle θ constant avec z, et effectue un mouvement de précession de fréquence ω_L autour de l'axe z.

Lors d'une expérience de RMN le champ $B_0 \approx 1-10$ Tesla est fixé une fois pour toute, et tous les moments magnétiques effectuent un mouvement de précession autour de z, avec une fréquence de Larmor qui leur est propre.

Pour manipuler les moments magnétiques on utilise un champ de radio-fréquences, de fréquence ω et d'intensité $B_1 \approx 10^{-2}$ Tesla. Pour que ce champ influence notablement un moment magnétique il faut régler sa fréquence sur la fréquence de résonance $\omega \approx \omega_L$. Dans ce cas le spin peut absorber ou émettre un quantum d'énergie $\hbar\omega$ précisement égal à la différence entre les niveaux d'énergie du moment magnétique dans le champ $\vec{B}_0$. Un basculement du spin autour des axes x et/ou y est réalisé en enclenchant le champ de radio-fréquences $\vec{B}_1(t) = (B_1 \cos\omega t, B_1 \sin\omega t, 0)$. L'hamiltonien est

$$H = -\frac{\hbar\omega_L}{2}\sigma_z - \frac{\hbar\omega_1}{2}(\sigma_x \cos\omega t + \sigma_y \sin\omega t).$$

Le calcul de l'opérateur d'évolution donne alors (si $\omega = \omega_L$)

$$\text{prob}(|\uparrow\rangle \to |\downarrow\rangle) = |\langle\downarrow |U(t)| \uparrow\rangle|^2 = \sin^2 \frac{\omega_1 t}{2}.$$

Nous voyons que la probabilité de transition oscille entre 0 et 1 avec une période égale à $\frac{2\pi}{\omega_1} \approx 10^{-6}$ sec. Ce sont les oscillations dites de Rabi.

Porte NOT. Si l'on pose $t = \frac{\pi}{\omega_1}$ (moitié d'une période de Rabi) on trouve

$$U(\frac{\pi}{\omega_1}) = \sigma_x = \text{NOT}.$$

Ainsi, pour réaliser une porte NOT il suffit d'enclencher le champ de radio-fréquences pendant une durée $\frac{\pi}{\omega_1}$. Cette opération, s'appelle aussi un π-pulse et retourne le spin $|\uparrow\rangle \to |\downarrow\rangle$ et $|\downarrow\rangle \to |\uparrow\rangle$.

Porte de Hadamard. Pour $t = \frac{\pi}{2\omega_1}$ (quart d'une période de Rabi) on trouve

$$U(\frac{\pi}{2\omega_1}) = H.$$

Pour réaliser une porte H il suffit d'enclencher le champ de radio-fréquences pendant une durée $\frac{\pi}{2\omega_1}$. Cette opération, s'appelle aussi un $\pi/2$-pulse et fait basculer un spin, initialement le long de z, dans le plan xy. $|\uparrow\rangle \to \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle)$ et $|\downarrow\rangle \to \frac{1}{\sqrt{2}}(|\downarrow\rangle - |\uparrow\rangle)$.

Autres portes. En theorie, on peut procéder de facon similaire pour réaliser d'autres opérations à un qubit, comme par exemple les rotations autour de z. Nous noterons qu'en pratique, vu la configuration des bobines, on ne peut pas créer des pulses de radiofréquences le long de z. Pour réaliser la rotation d'un qubit autour de z on utilise plutôt un déphasage des signaux ultérieurs sur ce

qubit, ce qui simule un rotation du référentiel autour de z. Ce déphasage dépend de la fréquence de Larmor du qubit en question.

Finalement il est important de noter que les pulses de radio-fréquences agissent sélectivement sur les qubits associés aux noyaux ^1H, ^{13}C, ^{19}F car les fréquences de Larmor sont bien separées. Nous verrons que cela est aussi possible pour des noyaux identiques car leur environnement chimique dans la molécule modifie légèrement leurs fréquences de Larmor.

10.3 Couplage spin-spin et portes à deux qubits

Les portes à deux qubits exploitent l'interaction naturelle entre moments magnétiques. L'évolution temporelle correspondant à cette interaction est un opérateur unitaire qui ne peut pas se ramener au produit tensoriel de deux unitaires à un qubit. En d'autre termes cette interaction crée de l'intrication et permet en particulier de réaliser la porte $CNOT$. Notons immédiatement que cela ne va pas sans poser de problèmes car cette interaction n'est pas enclenchable ou déclenchable à souhait. En effet elle est *naturelle* ! Ce problème peut être contourné grâce à la technique de *refocalisation* qui fait l'objet de la section suivante.

Pour deux moments magnétiques nucléaires dans la molecule, reliés par un axe $\vec{n}$ l'interaction dipolaire magnétique est de la forme

$$\hbar J_{\text{dip}}(3(\vec{\sigma}_1 \cdot \vec{n})(\vec{\sigma}_2 \cdot \vec{n}) - \vec{\sigma}_1 \cdot \vec{\sigma}_2).$$

La constante de couplage décroit comme l'inverse du cube de la distance entre moments magnétiques. Notez qu'il y a dans cette expression deux structures algébriques: le produit scalaire dans l'espace Euclidien et le produit tensoriel entre matrices de Pauli dans l'espace de Hilbert des spins. Ce premier terme ne joue pas de role dans un fluide car les rotations thermiques des molécules induisent un effet de moyenne sur le vecteur $\vec{n}$. En effet $\langle n_i \rangle = 0$ et $\langle n_i^2 \rangle = \frac{1}{3}$ $(i = x, y, z)$ entrainent

$$\langle (\vec{\sigma}_1 \cdot \vec{n})(\vec{\sigma}_2 \cdot \vec{n}) \rangle = \frac{1}{3} \langle \vec{\sigma}_1 \cdot \vec{\sigma}_2 \rangle$$

et donc l'interaction dipolaire magnétique s'annule en moyenne dans un fluide à l'équilibre thermique. Les moments magnétiques interagissent aussi avec le nuage électronique qui est dans leur environnement, ce qui entraine une interaction effective, à travers les liaisons chimiques, entre spin nucléaires. L'analyse[6] de ces effets est non-triviale et conduit à un hamiltonien de type Heisenberg (anisotrope)

$$\sum_{i,j=x,y,z} \hbar J_{ij} \sigma_{1i} \otimes \sigma_{2j}.$$

[6] Celle-ci fait appel à l'interaction de contact de Fermi entre le nuage électronique et le noyau, le principe de Pauli et la règle de Hund.

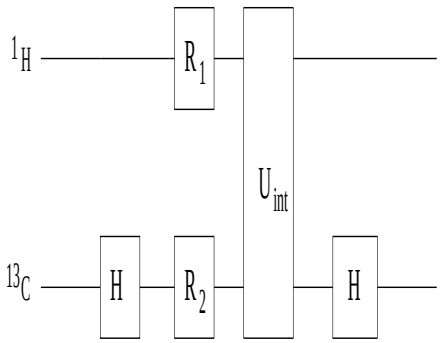


Figure 10.2 Circuit correspondant à l'identité pour la porte $CNOT$. Ici $U_{\rm int}$ est l'évolution unitaire due au couplage spin-spin. Les portes à un qubit sont réalisées grâce à des pulses de radiofréquences.

En fait $J_{ij} << \hbar\omega_L$ et cet hamiltonien peut être considéré comme une petite perturbation de l'hamiltonien de départ régissant la précession de Larmor, qui lui est diagonal dans la base computationelle. Un calcul de perturbation à l'ordre le plus bas montre alors qu'il suffit de retenir la composante z de cette interaction.

Tout compte fait, le couplage entre spins sera modelisé par (on posera $J_{zz} = J$)

$$\mathcal{H}_{int} = \hbar J \sigma_{1z} \otimes \sigma_{2z}.$$

L'évolution unitaire associée à cette interaction est

$$U_{int}(t) = \exp(-\frac{it}{\hbar}\mathcal{H}_{int}) = \exp(-itJ\sigma_{1z} \otimes \sigma_{2z}).$$

C'est une matrice 4×4 diagonale dans la base computationelle. Ses éléments diagonaux sont $e^{-itJ}; e^{itJ}; e^{itJ}; e^{-itJ}$. De plus $\hbar J << \hbar\omega_1$ ($<< \hbar\omega_L$). Cette séparation entre échelles d'énergies est très importante car elle signifie que *l'échelle de temps des interactions est mille fois plus grande que la durée des portes à un qubit*. En effet $\tau_{\rm int} \approx \frac{2\pi}{J} \approx 10^{-2}-10^{-3}$ sec, alors que $\tau_{\rm pulse} \approx \frac{2\pi}{\omega_1} \approx 10^{-6}$ sec. Ainsi le pas de temps élémentaire des calculs quantiques par RMN est de l'ordre de la millième de seconde. Cette échelle de temps n'est pas particulièrement faible, comparée aux échelles de temps des ordinateurs classiques; mais le gain potentiel du calcul quantique provient de la complexité potentiellement polynômiale des algorithmes, comparée à une complexité potentiellement exponentielle dans le cas classique.

L'identité suivante (exercice), et son circuit correspondant (figure 10.3), est à la base de la réalisation de la porte $CNOT$.

$$CNOT = (\mathbb{I} \otimes H)(R_1 \otimes R_2)U_{int}(t = \frac{\pi}{4J_z})(\mathbb{I} \otimes H)$$

ou

$$R_1 = \exp(i\frac{\pi}{2}\frac{\sigma_{1z}}{2}), \qquad R_2 = \exp(i\frac{\pi}{2}\frac{\sigma_{2z}}{2}).$$

Prenons l'exemple de la molécule de chloroforme, où les qubits sont les moments magnétiques des noyaux ^1H et ^{13}C. Supposons que ^1H est le qubit 1 et ^{13}C le qubit 2. Le protocole expérimental pour réaliser la porte $CNOT$ est le suivant:

- A l'instant initial, envoyer un $\frac{\pi}{2}$-pulse de fréquence $\omega = \omega_L^C$, dans le plan xy: cela réalise la porte de Hadamard sur le deuxième qubit. L'hamiltonien correspondant est
$$-\frac{\hbar\omega_1}{2}(\sigma_x \cos\omega_L^C t + \sigma_y \sin\omega_L^C t).$$
- Puis envoyer deux $\frac{\pi}{2}$-pulses de fréquences $\omega = \omega_L^H$ et $\omega = \omega_L^C$, dans la direction z: cela réalise les deux rotations R_1 et R_2 d'angle $\pi/2$ autour de z. L'hamiltonien correspondant est
$$-\frac{\hbar\omega_1}{2}\sigma_z(\cos\omega_L^H t + \cos\omega_L^C t).$$
- Attendre un temps $\tau = \frac{\pi}{4J}$. Pendant ce temps les deux qubits évoluent selon leur interaction naturelle d' hamiltonien
$$\hbar J\sigma_{1z} \otimes \sigma_{2z}.$$
- A l'instant final, envoyer un $\frac{\pi}{2}$-pulse, dans le plan xy, de fréquence $\omega = \omega_L^C$: cela réalise la dernière porte de Hadamard sur le deuxieme qubit. L'hamiltonien correspondant est le même que ci-dessus.

Bien sur, l'interaction naturelle $\hbar J\sigma_{1z} \otimes \sigma_{2z}$ agit aussi pendant les opérations sur les qubits individuels (les $\pi/2$-pulses). Donc ce protocole expérimental ne réalise la porte $CNOT$ qu'approximativement. Mais le point important est que cette approximation est excellente, dans la mesure où la durée des $\pi/2$ pulses est négligeable - et peuvent donc être considérés instantanés - par rapport à $\tau_{\text{int}} = \frac{\pi}{4J}$. Finalement, n'oublions pas qu'au cours de toutes ces opérations les spins effectuent leur précession de Larmor autour de la direction de $\vec{B}_0$.

10.4 Refocalisation

Considérons pour fixer les idées l'état obtenu après avoir effectuer le protocole du paragraphe précédent pour la porte $CNOT$. A priori cet état continue à évoluer avec l'interaction naturelle entre les moments magnétiques. Comment pouvons nous le préserver pendant un temps appréciable, disons de l'ordre de la millisecond ? Une autre situation d'intêret serait celle où nous voudrions effectuer des opérations sur certains qubits, tout en maintenant d'autres qubits dans un état donné pendant un temps de l'ordre de la milliseconde. A priori cela peut sembler difficile dans la mesure où les interactions naturelles ne peuvent pas être déclenchées à volonté. La technique de *refocalisation* permet de contourner le

problème. Celle-ci joue un role capital dans la réalisation expérimentale des algorithmes: en fait comme nous l'illustrons dans dernier le paragraphe, la plupart des opérations effectuées sont relatives á la refocalisation.

Soit $t_{\text{in}} < t_{\text{fin}}$ deux instants initiaux et finaux, tels que $t_{\text{fin}} - t_{\text{in}}$ soit de l'ordre de quelques millisecondes. Soit $|\psi_{\text{in}}\rangle$ l'état initial, d'un système de deux qubits, que l'on veut préserver. Son évolution naturelle le conduirait à l'état final

$$|\psi_{\text{fin}}\rangle = \exp\big(-i(t_{\text{fin}} - t_{\text{in}})J\sigma_{1z} \otimes \sigma_{2z}\big)|\psi_{\text{in}}\rangle.$$

Supposons maintenant qu'aux instants $\frac{t_{\text{fin}}+t_{\text{in}}}{2}$ et t_{fin} nous agissions avec un π-pulse correspondant à la rotation

$$R_{1x} = \exp(i\pi\frac{\sigma_{1x}}{2}) \otimes \mathbb{I}_2$$

d'angle π et d'axe x agissant sur le premier qubit (par exemple ${}^1H$). Comme ces pulses ont une durée négligeable par rapport à la durée totale de l'évolution, le nouvel état final - appelons le $|\psi_{\text{refoc}}\rangle$ - sera donné par

$$\begin{aligned}&|\psi_{\text{refoc}}\rangle\\ &\approx R_{1x}\exp\big(-\frac{i(t_{\text{fin}} - t_{\text{in}})}{2}J\sigma_{1z} \otimes \sigma_{2z}\big)R_{1x}\exp\big(-\frac{i(t_{\text{fin}} - t_{\text{in}})}{2}J\sigma_{1z} \otimes \sigma_{2z}\big)|\psi_{\text{in}}\rangle.\end{aligned}$$

Il n'est pas difficile de vérifier (exercice) l'identité mathématique exacte

$$\mathbb{I}_1 \otimes \mathbb{I}_2 = R_{1x}\exp\big(-i\frac{t}{2}J\sigma_{1z} \otimes \sigma_{2z}\big)R_{1x}\exp\big(-i\frac{t}{2}J\sigma_{1z} \otimes \sigma_{2z}\big),$$

valable pour tout t et J. Donc

$$|\psi_{\text{refoc}}\rangle \approx |\psi_{\text{in}}\rangle,$$

l'état obtenu par l'opération de refocalisation est une très bonne approximation de l'état initial (idéalement voulu).

Le principe général exposé ci-dessus peut être appliqué à des situations plus compliquées. En un mot, l'idée principale est de "corriger" la dynamique naturelle en agissant avec de courts pulses sur les qubits individuels.

10.5 Déplacements chimiques et effets de couplage

Il existe un effet important dont n'avons pas encore tenu compte: le déplacement chimique (ou chemical shift). Dans l'environnement de la molécule la fréquence de Larmor nue d'un noyau est modifiée par l'environnement chimique du noyau. En effet le champ local ressenti par un noyau est égal à B_0 plus des corrections diamagnétiques et paramagnétiques provenant du nuage électronique. Cela est important car des noyaux identiques auront des fréquences de Larmor légèrement différentes, ce qui permet de les adresser individuellement par les pulses de radiofréquences. Le décalage de ces fréquences de Larmor est appelé *déplacement chimique*.

Il y a encore un autre effet important sur les frequences de Larmor dont il faut tenir compte, qui provient du couplage spin-spin. Celui-ci entraine un "éclatement" de chaque fréquence de Larmor en plusieures fréquences satellites. Pour fixer les idées considérons à nouveau la molécule de chloroforme. Supposons que l'état du ^{13}C soit $|\phi\rangle$. Dans ce cas l'hamiltonien effectif de ^{1}H sera

$$\mathcal{H}_{\text{eff}} = -\frac{\hbar\omega_L^H}{2}\sigma_z^H + \hbar J_{HC}\sigma_z^H\langle\phi|\sigma_z^C|\phi\rangle.$$

Selon que $|\phi\rangle = |\uparrow\rangle, |\downarrow\rangle$ on obtient

$$\mathcal{H}_{\text{eff}} = -\frac{\hbar(\omega_L^H \pm 2J_{HC})}{2}\sigma_z^H$$

et on trouve deux fréquences de Larmor effectives pour ^{1}H. La fréquence de précession est $\omega_L^H - 2J_{HC}$ quand ^{13}C est dans l'état $|\uparrow\rangle$, et $\omega_L^H + 2J_{HC}$ quand ^{13}C est dans l'etat $|\downarrow\rangle$. De facon similaire le ^{13}C possède deux fréquences de Larmor $\omega_L^C - 2J_{HC}$ et $\omega_L^C + 2J_{HC}$ selon que ^{1}H est dans l'état $|\uparrow\rangle$ ou $|\uparrow\rangle$.

Considérons la molecule de trichloroétylène (figure 10.1). Les deux atomes de ^{13}C n'ont pas un environnement chimique identique si bien que les déplacements chimiques de leur fréquence de Larmor diffèrent. Cela est bénéfique car nous pouvons distinguer les deux qubits ! De plus chacunne de ces fréquences est éclatée à cause du couplage spin-spin. Il n'est pas difficile de voir que pour la molécule de trichloroétylène il y a *trois groupes de quatre fréquences*. En effet ω_L^H est éclatée en quatre fréquences satellites correspondantes aux quatres états possibles des deux C^{13}, $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$. De même ω_L^C est éclatée en deux groupes (un pour chaque carbone) de quatres fréquences chacun correspondantes aux quatre états des noyaux voisins. La figure 10.5 donne le spectre des deux ^{13}C. Les quatres fréquences de ^{1}H sont plus élevées et ne figurent pas sur cette échelle.

Il est facile de généraliser. Pour une molécule avec N noyaux de spin 1/2 (ou N qubits) il y a à priori N fréquences de Larmor (à cause du déplacement chimique ceci est le cas meme si les noyaux sont identiques). A cause du couplage spin-spin on aura en réalité N groupes de 2^{N-1} fréquences satellites[7]. Ces effets sont très important en spectroscopie par RMN. Les spectres moléculaires représentent une signature de la structure moléculaire, qu'il est souvent possible d'infèrer à partir des différents groupes de fréquences. Le nombre, la position et l'intensité des pics donnent de précieuses informations sur la molécule. En ce qui concerne les réalisatons expérimentales des algorithmes quantique, il faut tenir compte de cet effet pour régler avec assez de précision la fréquence des pulses. Il permet aussi comme indiqué plus haut de distinguer les qubits associés à des noyaux identiques. Nous allons voir dans le paragraphe suivant qu'il permet aussi de lire les états de la base computationelle.

[7] Ceci est vrai si tous les deplacments chimiques sont différents. Sinon certaines de ces fréquences satellites sont confondues.

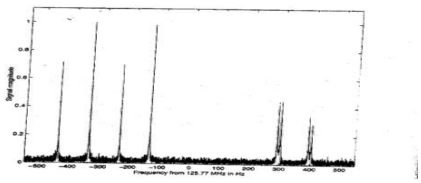


Figure 10.3 Spectre des deux ^{13}C dans la molécule de trichloroéthylène. L'origine des fréquences est placée à 125.77MHz et l'échelle horizontale est en Hz. [Source: Nielsen and Chuang, Quantum Computation and Information, CUP].

10.6 Lecture des qubits

Dans les expériences de RMN l'observation de l'état moléculaire est réalisé grâce à une mesure sur un ensemble statistique de qubits. Le signal obtenu est donc directement une valeur moyenne. Ainsi il ne s'agit pas vraiment de la mesure projective d'un état quantique individuel, mais plutôt d'une mesure collective. Bien sur, la valeur moyenne obtenue est conforme au postulat de la mesure.

Imaginons une expérience de RMN qui consiste à agir sur une solution moléculaire par une suite de pulses créés grâce à une bobine traversée par un courant alternatif. Cette même bobine va servir pour la mesure. L'état final des qubit $|\Psi_{\text{fin}}\rangle$ possède un moment magnétique total (dans ce paragraphe nous laissons tomber les facteurs de proportionalité et les constantes)

$$\vec{M}_{\text{fin}} \sim \langle\Psi_{\text{fin}}| \sum_{i=1}^{N} \vec{\sigma}_i \, |\Psi_{\text{fin}}\rangle.$$

Cette aimantation macroscopique précesse dans le champ $\vec{B}_0$ (autour de z) ce qui induit, en conformité avec la loi de Faraday, une tension et un courant dans la bobine (ici nous supposons que la bobine est orientée selon x et que sa résistance est R)

$$i(t) = RV(t) \sim -\frac{d}{dt} M_x(t).$$

Ce signal est une combinaison linéaire de signaux sinusoidaux de fréquences

égales aux différentes fréquences de Larmor constituant la précession de l'aimantation. Une analyse de Fourier donne un spectre de fréquences de Larmor (corrigées par les déplacements chimiques). Notons que le signal est exponentiellement décroissant sur une échelle $O(T)$, dans le domaine temporel, à cause des effets de relaxation de l'aimantation vers une valeur d'équilibre (décohérence). Dans le domaine fréquentiel cela se traduit par un élargissement $O(\frac{1}{T})$ des raies spectrales. Si cet élargissement est trop grand, c'est à dire la décroissance exponentielle du signal trop rapide, la mesure perd en précision.

Pour une seule fréquence on a

$$i(t) \sim e^{-t/T} \cos \omega_L t.$$

La raie spectrale correspondante est une fonction Lorentzienne

$$\hat{i}(\omega) \sim \frac{T}{1 + (\omega - \omega_L)^2 T^2}.$$

Appliquons ces principes à la lectures des états de la base computationelle. Nous n'allons pas tenir compte des effets de relaxation, dont la description dépasse le formalisme élémentaire utilisé ici. Commencons par le cas le plus simple d'un état à N qubits ayant tous la même fréquence de Larmor, et de la forme

$$|\uparrow\uparrow \cdots \uparrow\rangle.$$

Un $\pi/2$-pulse renverse cet état dans le plan xy,

$$|\Psi_{\text{fin}}\rangle = (|\uparrow\rangle + e^{-it\omega_L}|\downarrow\rangle) \otimes \cdots (|\uparrow\rangle + e^{-it\omega_L}|\downarrow\rangle)$$

(à une phase globale près). Cet état possède une aimantation macroscopique $(M_x(t), M_y(t), 0)$ précessant autour de z. Un calcul simple donne

$$M_x(t) \sim N \sin \omega_L t,$$

ce qui implique pour le courant sinusoidal traversant la bobine

$$i(t) \sim N\omega \cos \omega_L t, \qquad \text{et} \qquad \hat{i}(\omega) \sim N\delta(\omega - \omega_L), \omega > 0.$$

En commencant avec l'état initial $|\downarrow\downarrow \cdots \downarrow\rangle$ le $\pi/2$-pulse donne l'état $|\Psi_{\text{fin}}\rangle = (|\uparrow\rangle - e^{-it\omega_L}|\downarrow\rangle) \otimes \cdots (|\uparrow\rangle - e^{-it\omega_L}|\downarrow\rangle)$, et mène finalement a

$$M_x(t) \sim -N \sin \omega_L t$$

et

$$i(t) \sim -N\omega \cos \omega_L t, \qquad \text{et} \qquad \hat{i}(\omega) \sim -N\delta(\omega - \omega_L), \omega > 0.$$

Ces calculs simples permettent de tirer un enseignement intéressant.

- Un qubit dans l'état $|\uparrow\rangle$ donne des pics *positifs*[8].
- Un qubit dans l'état $|\downarrow\rangle$ donne des pics *négatifs*.
- Un qubit dans un état de superposition $\alpha|\uparrow\rangle + \beta|\downarrow\rangle$ donne un spectre avec des pics *positifs et negatifs*.

[8] En pratique on verra plusieurs pics a cause de l'effet du couplage avec les autres qubits.

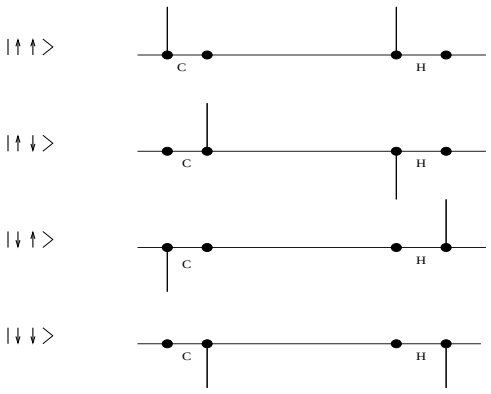


Figure 10.4 Représentation schématique des spectres de RMN correspondants aux états de la base computationelle du chloroforme (axe horizontal = fréquences de Larmor).

La figure 10.6 donne une représentation schématique des pics associés aux états de la base computationelle pour le cas de la molécule de chloroforme.

10.7 Réalisation de l'algorithme de Shor

Nous exposons ici les grandes lignes d'une expérience remarquable de Vandersypen-Steffen-Breyta-Yannoni-Sherwood-Chuang *"experimental realization of quantum factoring using nuclear magnetic resonance"*, Nature vol 414 pp. 883-887 (2001). Dans cette experience le nombre 15 est factorisé expérimentalement en suivant les principes de l'algorithme de Shor. En fait il s'agit de calculer la période de la fonction $f(x) = a^x \bmod 15$ pour a premier avec 15. Ces auteurs ont realisé l'expérience dans les deux cas $a = 11$ et $a = 7$. Ici nous allons illustrer cette expérience pour $a = 7$. Cette expérience, bien que ridicule du point de vue mathématique, est importante car elle prouve que les principes du calcul quantique peuvent être réalisés en laboratoire. D'autre part elle représente un tour de force de toute beauté.

Tout d'abord nous résumons la théorie de l'algorithme de Shor dans le cas concret qui nous intéresse ici.

La fonction $f(x) = 7^x \bmod 15$ est representée sur la figure pour les entiers $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, \dots\}$. Nous voyons que la période est $r = 4$ En d'autre termes l'ordre de 7 modulo 15 est égal a 4, un nombre pair. La factorisation est donc obtenue en calculant $\mathrm{PGCD}(7^{4/2} \pm 1; 15) = 3 \,\mathrm{et}\, 5$.

Pour voir la périodicité de cette fonction il suffit de travailler avec les entiers $\{0, \dots, 7\}$. Il faut trois qubit pour representer les kets associés $|x\rangle$. Ainsi nous prendrons $M = 2^3 = 8$. Nous avons aussi besoin de stocker les images $7^x \bmod 15$. Pour cela il faut au plus 4 qubits. Il nous suffit donc de travailler avec 7 qubits

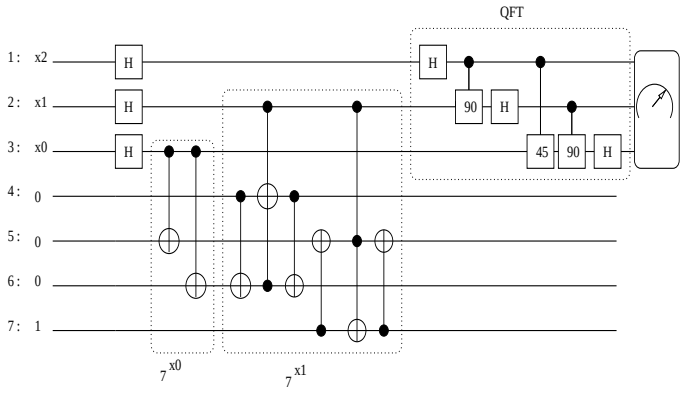


Figure 10.5 Circuit de l'algorithme de Shor pour $N = 15$ et $a = 7$. Les qubits numerotés de 1 à 7 correspondent aux spins des noyaux de la molécule de la figure **??**. Les bits $x_2x_1x_0$ représentent les entiers $x \in \{0, 1, \cdots, 7\}$. L'état entrant est $|000\rangle \otimes |0001\rangle = |0\rangle \otimes |1\rangle$.

au total. Notons aussi que si $x = x_0 + 2x_1 + 4x_2 + 8x_3$,

$$a^x = a^{x_0} a^{2x_1} a^{4x_2} a^{8x_3}$$

et donc pour $a = 7$ (puisque $7^4 = 1$)

$$7^x = 7^{x_0} 7^{2x_1}.$$

L'exponentielle modulaire est donc controllée seulement par les bits x_0 et x_1. Le circuit de Shor est donné sur la figure 10.7. Cette figure illustre aussi la réalisation des deux multiplications controllées par 7^{x_0} et 7^{x_1}. Celle-ci fait intervenir uniquement des portes $CNOT$ et nous laissons au lecteur le soin de vérifier que ce sont les circuits voulus.

Nous distinguons quatre phases dans l'évolution unitaire du circuit quantique. Cela sera pratique pour discuter l'expérience. Dans la phase (0) l'algorithme est initialisé dans l'état $|0000001\rangle$, qui correspond au produit tensoriel des "entiers" $|0\rangle \otimes |1\rangle$. La phase (1) correspond à l'action des portes de Hadamard qui prépare la superposition cohérente

$$\frac{1}{2^4} \sum_{x=0}^{7} |x\rangle \otimes |1\rangle$$

La troisième phase (2) correspond aux opérations d'exponentiation modulaire. L'état devient

$$(|0 + |4\rangle) \otimes |1\rangle + (|1\rangle + |5\rangle) \otimes |7\rangle + (|2\rangle + |6\rangle) \otimes |4\rangle + (|3\rangle + |7\rangle) \otimes |3\rangle.$$

Enfin dans la quatrieme phase (3) on applique la transformée de Fourier quantique qui donne l'état sortant

$$\textit{une superposition des etats } |0\rangle, |2\rangle, |4\rangle, |6\rangle \textit{ faites le calcul !}$$

Si nous appliquons maintenant le postulat de la mesure nous trouvons $\text{Prob}(y) = 1/4$ pour $y = 0, 2, 4, 6$ et $\text{Prob}(y) = 0$ pour $y = 1, 3, 5, 7$. On observe que $M/r = 2$. Puisque $M = 2^3 = 8$ on en déduit $r = 4$ ce qui est le bon résultat.

Ces dernières remarques indiquent que lors de la lecture de l'état sortant, par les techniques illustrées dans le pragraphe précédent, nous devrions observer des raies spectrales correspondantes aux états $|0\rangle = |000\rangle$, $|2\rangle = |010\rangle$, $|4\rangle = |100\rangle$, $|6\rangle = |110\rangle$. Discutons maintenant la réalisation expérimentale proprement dite.

Celle-ci utilise une solution contenant des molécules de synthèse contenant, entre autres, 7 noyaux actif de spin 1/2. Plus précisement il y a 2 C^{13} et 5 F^{19}. Une représentation schématique de la molécule est donnée sur la figure **??**, avec la numérotation utilisée pour les qubits. Les fréquences de Larmor deplacées ainsi que les couplages des 7 noyaux actifs peuvent être déterminés expérimentalement et sont donnés à titre d'indication dans la table. On peut penser à chaque molécule comme à un "circuit quantique" ou du moins un substrat pour le circuit.

La figure **??** montre la séquence de pulses utilisée pour réaliser les portes à un qubit, les portes à deux qubits étant réalisées de facon naturelle via les couplages spin-spin.

Sur cette figure les lignes de 1 a 7 représentent les 7 qubits (noyaux), l'axe horizontal représente le temps, et les barres verticales indiquent les instants auquels agissent les pulses. Comme expliqué plus haut la durée de chaque pulse est négligeable (de l'ordre de 10^{-6} sec) par rapport aux intervalles de temps séparant les pulses (de l'ordre de 10^{-3} sec) correspondant à l'évolution naturelle. On distingue 4 phases séparées par les lignes verticales pointillées. La phase d'initialisation (0) nécessaire à la préparation de l'état initial, la phase (1) de préparation de l'état de superposition cohérente, la phase (2) qui est la plus longue (d'une durée totale de $\sim$ 400 msec) calcule l'exponentielle modulaire, et enfin la phase (3) qui effectue la QFT (d'une durée de $\sim$ 120 msec). La durée totale de l'expérience est de 720 msec. Notons que la technique utilisée pour la préparation de l'état initial n'est pas triviale et fait partie des innovations de cette expérience. En effet, à priori l'état des 7 qubits, n'est pas l'état pur $|0000001\rangle$, mais un état de mélange thermique qui est ramené à un état "pseudo-pur" par des opérations appropriées. Cette étape constitue en fait une limitation importante pour réaliser le calcul quantique quand le nombre de qubits augmente. Nous n'en disons pas plus ici.

Donnons quelques informations supplémentaires sur les différents types de pulses utlisés. Les barres hautes rouges sont des $\pi/2$ pulses correspondant à des rotations autour des axes x positif (pas de croix), x negatif (croix inferieure), et y positif (croix superireure). Quand ces barres sont isolées elles représentent des portes de Hadamard alors que quand elles surviennent par paires elles sont separées par une évolution correspondant à une porte à deux qubits. Les barres bleu représentent les pulses utilisés pour la refocalisation. Ce sont des rotations d'angle π autour de l'axe x (positif $\rightarrow$ bleu foncé; négatif $\rightarrow$ bleu clair). Les petites barres vertent représentent des rotations autour de z.

On remarquera que la grande majorité des pulses utilisés ont trait á la refocalisation, et non pas aux portes du circuit quantique de Shor. La séquence de pulses nécessaires á la refocalisation a été calculée par simulations numériques, avant d'être implémentée dans l'expérience de RMN. De plus, un modèle de décohérence a été utilisé pour simuler la dynamique. Tous ces aspects dépassent de loin le cadre de cette introduction.

Passons finalement à l'étape finale qui consiste à lire *l'état sortant* des qubits. On utilise des $\pi/2$ pulses de lecture réglés sur les fréquences de résonance des 3 premiers qubits. Leurs spins basculent dans le plan xy et précessent autour de z, ce qui induit en vertu de la loi de Faraday, un signal dans la bobine. Le spectre de Fourier de ce signal est donné sur la figure **??**.

Ce spectre contient plusieures fréquences à cause des nombreux effets de chemical shift. Néanmoins on peut immédiatement en déduire que, dans l'état sortant, le qubit 0 était dans l'état $|\uparrow\rangle$ (c.à.d $|0\rangle$). D'autre part les qubits 1 et 2 sont dans des états de superposition de $|\uparrow\rangle$ et $|\downarrow\rangle$ (c.à.d $|0\rangle$ et $|1\rangle$). On peut donc en déduire que l'état sortant était une superposition de

$$|000\rangle,\ |010\rangle,\ |100\rangle,\ |110\rangle.$$

Les entiers intervenant dans cette superposition sont $|0\rangle$, $|2\rangle$, $|4\rangle$, $|6\rangle$, comme prédit par la théorie. Cela permet de conclure que $M/r = 2$ et donc $r = 4$, puisque $M = 2^3 = 8$.

Notes