Rapport de stage Licence Physique

L'information Quantique

Alexia Hocine

Tuteur : M. Pierre-Emmanuel Berche

9 Avril — 1er Juin 2018

Remerciements

Je tiens à remercier en premier lieu mon tuteur, Pierre-Emmanuel Berche, pour m'avoir permis de découvrir le GPM et la vie de chercheur. Je le remercie pour son écoute et son accompagnement dans mes recherches et la rédaction de ce rapport, sur le sujet fascinant de l'information quantique. Ce stage m'aura aidé à comprendre une des applications de la physique quantique, ce qui je pense m'accompagnera dans la suite de mon parcours.

Je souhaite remercier aussi la post-doctorante Amjaad Abou Latif qui m'a consacré du temps afin de m'expliquer le sujet de ses recherches, et qui m'a conseillé plusieurs lectures, qui m'ont aidé à comprendre les méthodes de résonance magnétique nucléaire et découvrir certaines méthodes de fabrication de qubits.

Plus généralement, je remercie les enseignants de l'université de Rouen-Normandie pour leurs accompagnements durant ces années de licences, ce qui m'a permis de pouvoir aborder ce sujet de stage par le biais de la physique et de l'informatique. Et je souhaite remercier le GPM qui m'a accueilli et immergé dans le monde dédié à la recherche au cours de ces 2 mois.

Recherche de stage

Dans un premier temps, je souhaitais faire un stage en astrophysique. C'est pourquoi, j'ai postulé auprès de l'enseignant-chercheur Jean-François Donnati de l'université de Toulouse.

Mais mon projet professionnel évoluant, je commençais à me tourner vers des chercheurs en physique théorique. Lorsque j'ai reçu par mail la proposition de stage de M. Berche sur l'information quantique, ce sujet m'a toute suite plu car il allie à la fois les notions de physique et d'informatique. Et il allait me permettre d'appliquer et d'approfondir mes notions de physique quantique étudiées au cours de l'année.

Je suis alors passée au bureau de M. Berche afin d'en parler directement avec lui et qu'il m'explique le projet plus en détails. Suite à cette entretien, je lui ai communiqué mon CV et une lettre de motivation. Après plusieurs jours, il m'a attribué ce stage.

Résumé

Le but de ce rapport est d'expliquer les fondamentaux de l'information quantique, d'expliquer son intérêt, ses avantages, ses limites et de donner un aperçu des avancées dans ce domaine.

En effet, il s'agit d'un sujet qui suscite énormément de recherches ces dernières années dans des secteurs très hétéroclites (telles que la physique, les mathématiques, l'informatique, et l'électronique). Pour des applications toutes aussi vastes, comme la physique des matériaux, la physique subatomique, la chimie, la médecine, l'intelligence artificielle, la finance. Ce qui suscite l'intérêt, la recherche et donc des financements et ainsi aider au développement de la recherche.

Ainsi au cours des dernières années plusieurs récompenses ont été attribuées dans ce domaine notamment le prix Nobel de physique de 2012 attribué à Serge Haroche et David Wineland sur la manipulation et l'analyse de particules quantiques non destructives.

Abstract

This intership report's goal is to explain the basis of quantum information, especially its advantages and limitations and finally to give an overview of steps made in this field.

Indeed, it is a topic which creates a lot of research field in many areas such as physics, mathematics, computing and électronic since few years. Quantum information also has a lot of applications for example in material's physics, subatomic physics, chemistry, medecine, artificial intelligence or also in finance. This amount of application fields arouse the interest of researchers and financial support which helps to developp research.

That's why, the grateful reward the Nobel Price was given in 2012 in the field of quantum information thanks to reaserch done on manipulation and analysis of non destructives quantum particles.

Table des matières

Introduction

Introduit dans les années 80 par Feynman pour palier aux problèmes qu'ont les ordinateurs dits classiques pour simuler les situations quantiques, l'information quantique fait de plus en plus rêver les chercheurs et les industriels grâce aux phénomènes quantiques étranges comme la téléportation, la superposition et l'intrication d'états.

De plus avec la fin de la loi de Moore certains voient dans ce domaine d'étude l'avenir du numérique, à l'instar du projet européen d'Atos soutenu par Serge Haroche (professeur au Collège de France et prix Nobel 2012 de physique), Artur Ekert (professeur de physique quantique à l'Institut de Mathématiques, Université d'Oxford et de Singapour), Cédric Villani (professeur à l'Université Claude Bernard (Lyon I), directeur de l'institut Henri Poincaré CNRS/UPMC et médaille Fields)et David DiVincenzo (professeur à la fondation Alexander von Humboldt et directeur de l'institut de nanoélectronique théorique au centre de recherche Jülich.)

Pour commencer cette étude, nous rappellerons les notions de physique quantique utilisées dans l'information quantique comme la dualité des particules, les principes de superposition et d'intrication d'états, et on introduira la notion de cohérence quantique.

Ensuite nous aborderons les concepts informatiques nécessaires pour avoir un aspect général de ses perspectives, afin d'entrevoir les avantages de ce genre de technologie.

Et dans un dernier temps, j'expliquerai les différents types de réalisations physiques d'ordinateurs, et certaines pistes de recherches, où on abordera aussi les recherches effectuées au GPM en collaboration avec l'IPCMS de Strasbourg, ainsi que des avancées en matière de simulations numériques.

Chapitre 1

Généralités

Inventé par Jonh Von Neumann, le **processeur** est le composé électronique qui exécute les instructions élémentaires, qui agit sur les bits par l'intermédiaire des circuits intégrés.

Aujourd'hui on parle plutôt de **microprocesseurs**. Inventé en 1969 par Marcian Hoff et Federico Faggin, il s'agit d'une version compacte et réduite, en un seul circuit intégré, d'un processeur. Intel en commercialise depuis 1971.

En 1965, en observant les avancées rapides de cette technologie, Gordon Earle Moore (cofondateur de Intel) prédit que le nombre de transistors par circuit doublerait chaque année à coût constant. Ce qui augmenterait la puissance de calculs des nouveaux ordinateurs. Cette conjoncture est appelé la **loi de Moore**. Elle a un peu évolué avec le temps, dans un 2e temps on parlait de 18 mois, puis tous les 2 ans [1]. Mais cette conjoncture a été auto-réalisatrice, puisque tous les constructeurs se sont entendus sur cet objectif.

Ainsi dans le tableau ci-dessous, on peut remarquer la progression fulgurante des microprocesseurs d'Intel.

Date de commercialisation	Nom du microprocesseur	Nb transistors	Finesse de la gravure en *nm*	MIPS
1971	Intel 4004	2 300	10 000	0,06
1982	Intel 80286	1 200 000	1 000-800	1
1993	Pentium	3 100 000	800-250	100
2004	Pentium 4D	125 000 000	90-65	9 000
2015	Intel Core (Skylake)	1 750 000 000	14	

FIGURE 1.1 – Exemples de microprocesseurs

MIPS : nombre en millions instructions par seconde.

On remarque que les microprocesseurs ont de plus en plus de transistors grâce à une gravure de plus en plus précise. Cette miniaturisation leur fait gagner en rapidité de traitement des calculs.

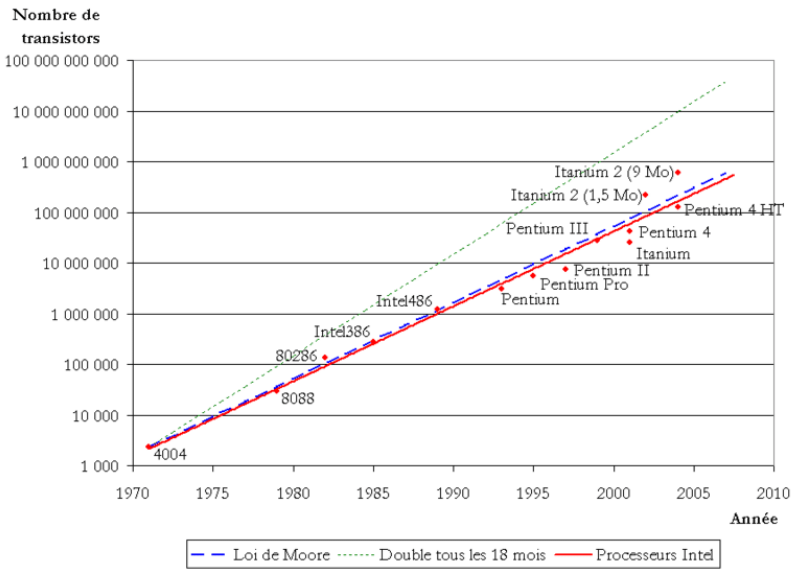

FIGURE 1.2 – Nombre de transistors en fonction du temps

Mais dès cette annonce, G. Moore avait conscience de la limite liée aux phénomènes quantiques.

Aujourd'hui, cette conjecture est de moins en moins vraie. Il est de plus en plus difficile de continuer à réduire la taille des transistors. En 2015, les composants ont atteint 14 nm. On arrive donc à construire des transistors à l'échelle d'une centaine d'atomes de largeur. Mais les composants s'échauffent beaucoup et des comportements quantiques non désirés apparaissent. Comme des manifestations de l'effet tunnel, c'est-à-dire des électrons qui changent de transistors, ce qui provoque des pertes de données et des erreurs de calculs très importantes, et qui nécessitent des algorithmes de corrections d'erreurs plus compliqués. Cette situation ralentit le rythme de cette miniaturisation et augmente les coûts de production.

Cette situation n'est pas forcément négative, elle pousse à la re-fondation du numérique par la qualité. En effet, avec l'augmentation constante des performances des ordinateurs, toute l'industrie informatique n'a pas été très consciencieuse. Comme la puissance de calcul et de stockage augmentaient continuellement, les développeurs pouvaient se reposer sur la prochaine génération de composants pour négliger l'optimisation de leurs codes. Ce qui engendre des programmes plus gourmands en temps de calculs et en espace mémoire que nécessaire. Et comme la programmation est empirique, ces négligences se sont accumulées au cours des générations de logiciels.

Les industriels réfléchissent aussi à d'autres méthodes pour augmenter la puissance de calcul. Par exemple la mise en parallèle de plusieurs processeurs, ce qui multiplie le nombre de tâches effectuées par seconde. Ainsi, même si le processeur n'évolue pas, la puissance augmente et donc l'ordinateur est plus rapide, mais aux dépends de la taille et du nombre de composants.

De plus cette stagnation devrait permettre une diminution des coûts de production, donc du prix de vente et une démocratisation du numérique. Avec de nouveaux matériaux et des processus plus légers, cette mutation va permettre de diminuer le coût énergétique. Il s'agit d'un problème de plus en plus important avec l'augmentation des utilisateurs et l'explosion des données à stocker, il faut toujours plus de ressources, de stockage et d'énergie.

D'une idée bizarre dans les années 80, l'ordinateur quantique devient de plus en plus concret, intéressant, voire inquiétant. Ce domaine de recherche a été ouvert en 1982 par Richard Feynman. Il voulait utiliser les phénomènes quantiques de superposition et d'intrication pour effectuer des calculs complexes plus rapidement qu'avec n'importe quelle ordinateur dit classique.

Aujourd'hui de nombreux acteurs privés et publiques investissent dans le développement de l'**information quantique**. Car, ce n'est pas seulement la suite logique à la fin de la loi de Moore, l'information quantique ouvre de nouvelles perspectives, notamment dans la résolution des calculs complexes. Ce qui est aussi un problème de sécurité mondial, car la cryptographie est basée sur des problèmes mathématiques difficiles et longs à résoudre pour nos calculateurs classiques.

Mais les applications potentielles permettraient des avancées majeures dans les domaines économiquement importants telle que l'intelligence artificielle, la recherche, le transport, la finance, la simulation numérique, la sécurisation de l'informatique...

L'information quantique cherche à utiliser des phénomènes de la physique quantique pour révolutionner le numérique. En effet à l'échelle atomique et subatomique, les particules ont des comportements surprenants et contre intuitifs. Elles ont l'air de ne plus obéir aux lois de la physique classique. En effet les particules peuvent se trouver à plusieurs endroits au même moment, ou semble diffuser leurs changements d'états à des vitesses supérieurs à celle de la lumière.

L'idée de l'information quantique est d'utiliser ces propriétés quantiques dans le monde du numérique.

1.1 Les bases de la physique quantique

La majorité de ces principes ont été posés au début du XX^{e}siècle.

Pour commencer, en 1900, Max Planck introduit la notion de **quanta** pour expliquer mathématiquement le rayonnement thermique d'un métal chauffé. Car la loi classique de Rayleigh-Jeans diverge à basse fréquence, contrairement l'expérience. C'est ce que Paul Ehrenfest a appelé la **catastrophe ultraviolette**.

Les courbes à gauche sont des représentations de la loi de Planck à différentes températures et à droite est représentée celle de Rayleigh-Jeans. Toutes 2 sont des distributions spectrales en fonction de la longueur d'onde. On constate que la loi classique est une approximation de la loi quantique aux grandes longueurs d'onde. La physique classique ne permet pas d'expliquer la distribution spectrale d'un corps.

Ainsi la loi de Rayleigh-Jeans est une approximation de la loi de Planck, lorsque $\lambda >> \frac{hc}{kT}$.

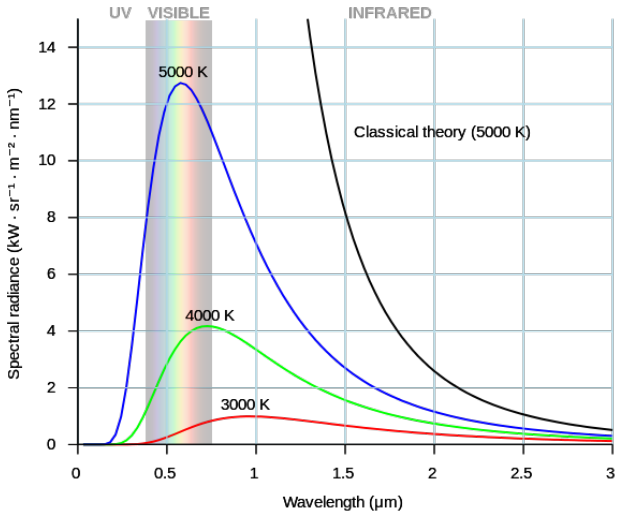

FIGURE 1.3 – Loi de Planck quantique - Loi de Rayleigh-Jeans classique

Bien que la notion de quanta soit pour M. Planck une réponse purement mathématique, elle impose que les échanges d'énergie entre la lumière et la matière ne peuvent prendre que certaines valeurs qui sont donc **quantifiées**. En effet, en physique quantique certaines valeurs sont quantifiées, c'est-à-dire qu'il n'existe que certaines valeurs possibles.

En 1905, pour expliquer l'effet photo-électrique, c'est-à-dire le fait qu'un métal perd des électrons si la fréquence de la lumière est suffisante, Albert Einstein décrit la lumière comme des grains transportant une énergie proportionnelle à sa fréquence.

À l'époque un débat existe sur la nature de la lumière, avec 2 courants distincts. Les partisans de Isaac Newton considèrent la lumière comme des **petits corpuscules** et ceux de Christian Huygens qui l'imaginent comme ondulatoire. Mais pour A. Einstein la lumière a un caractère dual, c'est-à-dire que la lumière est à la fois une particule et une onde, selon les conditions expérimentales.

En 1913, Niels Bohr en déduit que si seulement certaines valeurs de l'énergie sont possibles, alors les électrons ne peuvent être que sur certaines orbites (dans une représentation planétaire de l'atome). Et que l'électron peut changer d'orbite uniquement par saut quantique, ce qui produit l'émission ou l'absorption d'un photon. Donc une perte ou un gain d'une certaine énergie :

$$E = h\nu$$

E : énergie en J
h : constante de Planck ($h \approx 6,626\ 070\ 040.10^{-34}\ J.s$)
ν : fréquence en Hz

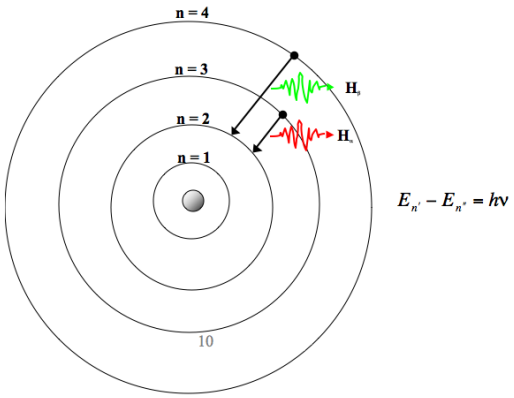

FIGURE 1.4 – Modèle de l'atome de Bohr

En 1923, Louis de Broglie postule que les particules de petites tailles, comme les électrons, sont aussi de nature

duale. Ce qui lui a valu le prix Nobel de Physique de 1929. Ce résultat fut mis en évidence expérimentalement par Davisson et Germer avec la diffraction d'électrons sur du nickel.

$$\lambda = \frac{h}{mv}$$

λ : longueur d'onde en m
h : constante de Planck ($h \approx 6,626\ 070\ 040.10^{-34}\ J.s$)
m : masse en kg
v : vitesse en $m.s^{-1}$

Enfin de 1925 à 1926, Heisenberg, Schrödinger et Dirac retranscrivent toutes les observations physiques : la dualité, la superposition, l'indéterminisme... en mathématiques et écrivent les bases de la théorie quantique.

1.2 La dualité onde-corpuscule

En 1905 puis 1923, Albert Einstein et Louis de Broglie montrent que la lumière et les atomes peuvent avoir tantôt un comportement corpusculaire, tantôt un comportement ondulatoire. Pour expliquer ce comportement contradictoire on peut utiliser l'expérience des trous d'Young.

Au cours du XIX^{e} siècle, Thomas Young cherche à étudier le comportement de la lumière. En 1801, il met au point une expérience d'optique. Il place une source lumineuse et un écran photovoltaïque séparés par un écran perforé par un seul trou et un second écran perforé par 2 trous identiques. Si la lumière se propage en ligne droite, on devrait observer 2 disques nets lumineux correspondant aux 2 trous de l'écran.

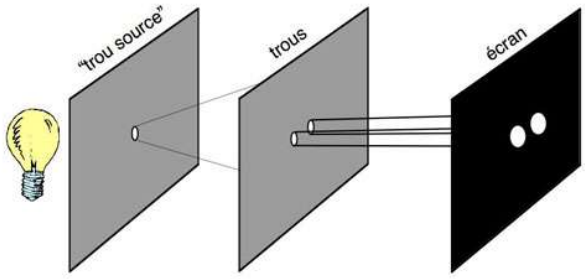

FIGURE 1.5 – Expérience des trous d'Young (1801) : dispositif

Or si les trous sont suffisamment petits (par rapport à la longueur d'onde de la lumière), on observe sur ces taches des bandes lumineuses et sombres, c'est-à-dire des bandes d'interférences.

À certains endroits de la plaque, la lumière interfère de manière constructive, on observe alors une frange brillante. Sinon la lumière interfère de manière destructive, on observe alors une frange sombre.

Cette expérience met en évidence le **caractère ondulatoire** de la lumière.

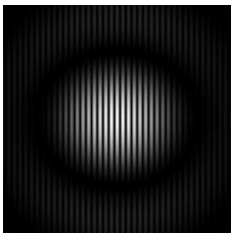

FIGURE 1.6 – Expérience des trous d'Young : Résultat expérimental

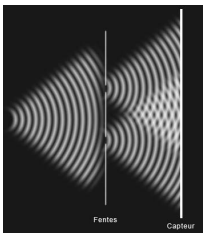

FIGURE 1.7 – Expérience des trous d'Young, propagation ondulatoire

En 1961, Claus Jönsson effectue la même expérience avec des électrons et obtient les mêmes résultats que T. Young. Les électrons peuvent manifester un comportement ondulatoire, malgré leur **nature corpusculaire**.

En effet, si on diminue la fréquence de collisions des particules (photons ou électrons) sur la plaque photovoltaïque, on observe des collisions individuelles, donc l'**aspect corpusculaire** de ces particules. Mais aux temps longs, avec le grand nombre de collisions, des franges d'interférences se forment et exposent l'**aspect ondulatoire** des particules.

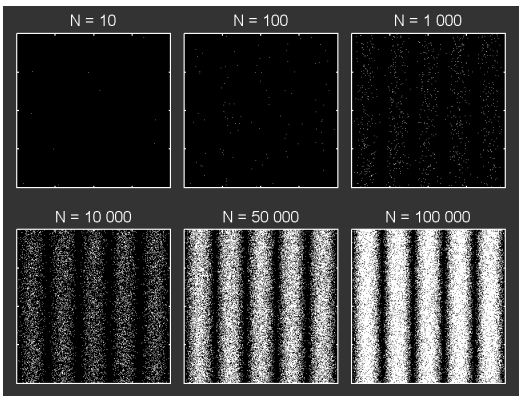

FIGURE 1.8 – Expérience des trous d'Young, variation du nombre de particules

Ce phénomène met en évidence un paradoxe : la lumière et les électrons... sont en même temps une onde et des particules. En réalité, on ne peut donc pas dissocier l'aspect corpusculaire et ondulatoire des particules.

Toujours dans le cadre des trous d'Young, on ne sait pas où une particule isolée va frapper la plaque. Mais on connait les probabilités de collisions en fonction de la position sur la plaque, plus élevée au niveau des franges brillantes. Ainsi, deux particules émises au même endroit d'une source, peuvent frapper la plaque à deux endroits différents. On perd la notion de trajectoire et de déterminisme de la physique classique. Car à partir de conditions initiales identiques, leurs destinations sont inconnues, probabilistes.

Cependant, avec un grand nombre de particules individuelles, l'apparition des franges est parfaitement anticipée. Ce qui permet de retrouver le déterminisme classique que l'on retrouve à l'échelle macroscopique.

De plus, pour savoir par quelle fente passe le photon, on place un photo-multiplicateur derrière l'une des 2 fentes. Donc soit le photon est absorbé, soit il passe par l'autre fente. On connait alors la fente par laquelle passe chaque photon, mais comme les photons d'une des 2 fentes ne passent plus, nous perdons la figure d'interférence. Donc pour connaître la trajectoire de tous les photons qui frappent la plaque, on perd l'aspect ondulatoire.

En 1927, Heisenberg démontre qu'il est impossible de connaître avec une précision infinie, la position et la quantité de mouvement d'une particule simultanément. Ce principe d'incertitude est synthétisé mathématiquement par :

$$\Delta x \Delta p \geq \frac{\hbar}{2} \tag{1.1}$$

Δx : précision sur la mesure de la position
Δp : précision sur la mesure de la quantité de mouvement
$\hbar$: constante de Planck réduite ($\hbar = \frac{h}{2\pi} \approx 1,054\ 571\ 800.10^{-34}\ J.s$)

Ainsi au niveau macroscopique, les expériences sont parfaitement déterministes grâce aux probabilités sur un très grand nombre de particules (des milliards). Mais au niveau microscopique, on ne peut pas savoir à l'avance le comportement d'une particule, puisque si on effectue une mesure, on perturbe fondamentalement le système.

1.3 Le principe de superposition

En physique classique à chaque instant, les objets ont des caractéristiques bien définies : position, vitesse, énergie... Alors qu'en physique quantique les objets peuvent avoir une infinité d'états possibles, c'est-à-dire qu'ils peuvent, au même moment, être à plusieurs endroits, avoir plusieurs vitesses, ou encore des niveaux d'énergie différents...

Mathématiquement, en 1926, Erwin Schrödinger associe chaque particule en mouvement à un paquet d'ondes, c'est-à-dire une superposition d'ondes concentrées dans l'espace. Il le représente par une **fonction d'onde** Φ solution de l'équation d'onde.

$$i\hbar \frac{\partial}{\partial t}\Phi(r,t) = \underbrace{-\frac{\hbar^2}{2m}\,\Delta\Phi(r,t)}_{\text{énergie cinétique}} + \underbrace{V(r)\ \Phi(r,t)}_{\text{énergie potentielle}} \tag{1.2}$$

En 1935, pour aider à la compréhension de cette propriété quantique, Schrödinger imagine une expérience de pensée, dans laquelle on mettrait un chat dans une boîte avec une fiole de poison et un élément radioactif. Le dispositif serait placé de telle façon que dès que l'élément radioactif se désintègre la fiole se brise et le chat meurt.

Tant que la boite est fermée, on ne sait pas si la fiole s'est brisée, on ne sait donc pas si le chat est vivant ou mort. Schrödinger considère que le chat est mort et vivant. Il est dans les 2 états simultanément.

Mathématiquement, on écrirait cette superposition d'états tel que :

$$|Chat\rangle = \alpha|Mort\rangle + \beta|Vivant\rangle$$

où α et β sont les amplitudes qui peuvent varier avec les conditions expérimentales. Ici l'élément est radioactif donc ils varient avec une décroissance exponentielle.

Mais dès qu'on ouvre la boîte, on voit si le chat est vivant ou mort. On lève l'incertitude, on effectue une mesure. Donc on sait si le chat est mort, ou vivant.

Comme ici pour le chat, les particules sont dans une superposition d'états jusqu'à ce que l'interaction avec l'environnement extérieur projette le système sur l'un des états possibles. Il n'en reste alors plus qu'un et le système devient classique.

En physique quantique, une particule est représentée par une fonction d'onde qui est la superposition de plusieurs états, donc elle peut prendre n'importe lequel de ces états. Lorsqu'on effectue la mesure, la fonction d'onde se réduit, la particule prend une des valeurs possibles aléatoirement et l'objet devient classique.

Donc si on ne mesure pas une propriété (spin, polarisation, énergie...), l'objet quantique est dans un état de superposition de plusieurs états à la fois. Mais dès que l'on effectue la mesure, la superposition quantique disparait, et l'objet n'a plus qu'un seul état possible.

Mathématiquement, on représente un système quantique $|\Psi\rangle$ par un vecteur de l'espace de Hilbert de la base $\{|0\rangle, |1\rangle\}$.

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

avec les coefficients de probabilité $\alpha, \beta \in C$ sachant $|\alpha|^2 + |\beta|^2 = 1$ car $|\Psi\rangle$ doit être normalisé.

Comme une particule peut être à plusieurs endroits à la fois, on ne peut pas dire quelle est sa trajectoire. Richard Feynman explique que la particule passerait par tous les chemins qu'il lui est possible de prendre. Et donc la bonne trajectoire est l'intégration sur tous les chemins possibles.

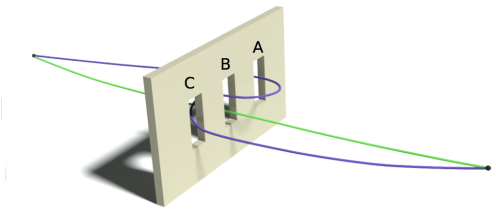

FIGURE 1.9 – On considère qu'une particule quantique passe en même temps par tous les chemins qui lui sont permis

Avec la superposition quantique on explique aussi l'indéterminisme des mesures. En effet, en physique quantique on ne peut pas dire quel est le niveau d'énergie d'une particule puisqu'elle peut en occuper plusieurs simultanément.

Alors qu'en physique classique on peut prévoir à partir de données l'état d'un système, en physique quantique on ne le peut plus. Mais on peut déterminer quelles sont les probabilités pour chaque état.

La perte de la superposition d'un objet quantique est appelé la **décohérence quantique**. En effet, lorsqu'un objet quantique interagit avec son environnement (particules, rayonnement, champs électrique ou magnétique) ses caractéristiques quantiques vont progressivement s'atténuer jusqu'à ne plus être mesurables et disparaitre. Et comme les objets macroscopiques, qui mettent en jeux un très grand nombre de particules sont constamment en interaction avec les autres particules, la lumière ou d'autres facteurs perturbateurs, ils n'ont plus leurs caractéristiques quantiques. Ces interactions ont les mêmes effets qu'une mesure pour un objet quantique. C'est à cause de cette décohérence que nous n'observons pas d'objet quantique dans notre quotidien macroscopique.

C'est pourquoi, pour observer un objet quantique, on doit se placer dans les conditions du laboratoire pour contrôler l'environnement et atténuer la décohérence, c'est-à-dire dans un environnement vidé de ses particules, opaque et à des températures proches de $0K$.

1.4 L'intrication quantique

En physique quantique, on peut former des systèmes avec plusieurs objets quantiques de même nature (électrons, photons...). On ne peut pas décrire un objet intriqué sans l'autre. Ces systèmes restent liés même si on les sépare spatialement. Cette intrication implique que si on effectue une mesure sur l'un alors immédiatement l'autre prendrait une valeur déterminée. Par exemple, si on intrique un électron et un positron alors ils auront des spins opposés après la mesure, respectant ainsi le principe de Pauli [2].

Donc quelle que soit la distance qui sépare 2 particules intriquées, si on mesure une propriété pour l'une, l'information sera instantanément mesurable sur la seconde particule.

En 1935, Einstein, Podolsky et Rosen publient un article intitulée *Can quantum-mechanical description of physical reality be considered complete ?* [3]. Pour eux, le principe d'intrication avait plusieurs incohérences, ils refusaient la séparabilité et la localité d'un système intriqué.

En effet, selon la relativité restreinte, la **théorie locale** dit que pour qu'il y ait un lien de causalité entre 2 évènements, le temps qui les sépare doit être inférieur au temps mis par la lumière pour transiter entre eux. Or si l'un des 2 photons subit une mesure alors l'information sera immédiatement perçue par le second. La distance n'a donc aucune influence, et ce lien ne subit aucun retard. Donc cette mesure se propage plus vite que la vitesse de la lumière. Ce qui viole l'une des conditions fondamentales de la relativité restreinte et le **principe de localité** d'après Einstein, Podolsky et Rosen. C'est ce qu'on appelle le **paradoxe EPR**.

Ils supposent que la théorie de la physique quantique est incomplète et qu'il existe des *variables cachées*. Elles contiendraient les informations manquant pour rendre la physique quantique déterministe et non probabiliste. Pour eux l'état de la mesure est prédéterminé lors de l'intrication du système et la mesure ne fait que révéler un état déjà existant.

Mais d'autres, comme Niels Bohr, expliquent que cette intrication est indépendante des positions des particules, car elle n'est pas locale, ce qui ne contre-dit pas la relativité restreinte, puisque aucune information n'est transmise.

Ce débat a été considéré par les contemporains comme philosophique ou épistémologique, car la théorie quantique fonctionne expérimentalement. Cependant, il s'agit de la validation de la physique quantique et de ses principes fondateurs.

En 1964, en cherchant à valider expérimentalement le paradoxe EPR, John Stewart Bell démontre une inégalité mathématique inviolable si la physique quantique est déterministe, appelée **les inégalités de Bell**.

On se place dans la théorie réaliste locale EPR. Donc si l'inégalité n'est pas vérifiée, alors cette théorie est fausse. Mathématiquement, on peut trouver certains cas où elle ne fonctionne pas, toute la question était de les vérifier expérimentalement pour valider ou non la théorie EPR ou quantique.

En 1982, l'**expérience d'Alain Aspect** (université d'Orsay) parvient à violer cette inégalité expérimentalement, ce qui démontre le caractère local de la physique quantique, prouve son indéterminisme et invalide la théorie des variables cachées.

Chapitre 2

L'informatique quantique

2.1 Le bit quantique - Le qubit

Le bit quantique, appelé **qubit**, est le support élémentaire de l'information quantique. Un bit classique a 2 états possibles, représentés par 0 ou 1. Grâce au principe de superposition quantique, un qubit est dans une superposition de ces 2 états, autrement dit dans une combinaison linéaire de ces 2 états, c'est-à-dire une infinité d'états différents.

Mathématiquement, un qubit $|\psi\rangle$ est un vecteur unitaire de la base de Hilbert en 2 dimensions [2] :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$\text{avec } \alpha, \beta \in \mathbb{C} \text{ où } |\alpha|^2 + |\beta|^2 = 1$$

Graphiquement, nous pouvons représenter ces qubits dans une **sphère de Bloch**. Il s'agit d'une sphère unitaire, fonctionnant sur un principe analogue au repère sphérique. Il faut alors considérer les angles $\theta \in [0, \pi]$ et $\phi \in [0, 2\pi]$ pour définir la position de l'extrémité de $|\psi\rangle$ dans la base orthonormée $\{|0\rangle, |1\rangle\}$. Et notre qubit s'écrit cette fois [2] :

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

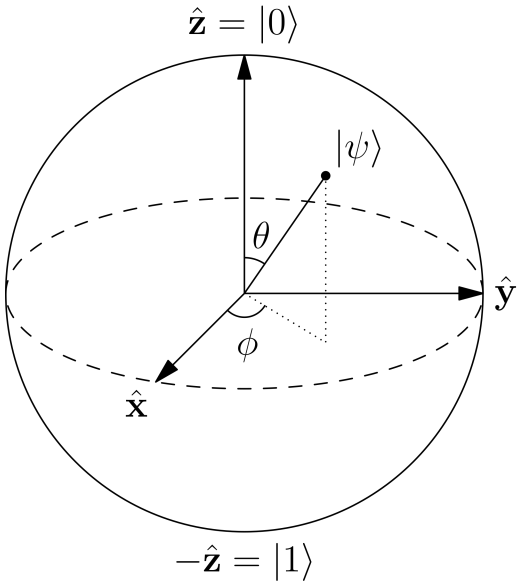

FIGURE 2.1 – Sphère de Bloch

Si on effectue la mesure d'un qubit, on obtiendra un résultat analogue à un bit classique : soit 0, soit 1. Mais, alors que la valeur d'un bit est définie, le qubit ne le sera qu'à la mesure et aura une probabilité de $|\alpha|^2$ d'être dans l'état 0 et $|\beta|^2$ dans l'état 1.

2.2 Clonage quantique

2.2.1 Principe de non-clonage

Mathématiquement, le clone parfait d'un état quantique est caractérisé par : $\forall|\psi\rangle$,

$$|\psi\rangle \rightarrow |\psi\rangle|\psi\rangle$$

($|\psi\rangle|\psi\rangle$: entre les 2 qubits on effectue l'opération du produit tensoriel).

En 1982, William Kent Wootters et Wojciech Hubert Zurek démontrent qu'il est impossible d'obtenir une fidélité égale à 1 [4, 2].

Supposons un état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ que l'on souhaite cloner.

$$\begin{aligned}|\psi\rangle|\psi\rangle &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle\end{aligned}$$

Donc en souhaitant cloner l'état $\alpha|0\rangle + \beta|1\rangle$ on doit obtenir l'état $\alpha^2|00\rangle + \beta^2|11\rangle$. Ce qui implique que $\alpha\beta = 0$, donc que α ou β soit nul. Donc $|\psi\rangle = |0\rangle$ ou $|\psi\rangle = |1\rangle$, c'est-à-dire sans superposition. Il est donc impossible de cloner un état quantique [2].

En effet, si on veut recopier un objet quantique, on doit effectuer une mesure, ce qui lui fera perdre la superposition quantique et dégradera l'information.

2.2.2 Application pour la cryptographie

En appliquant à ce principe de non clonage au domaine de la cryptographie, on peut sécuriser les clés privées.

En effet, les protocoles de la cryptographie classiques reposent sur des problèmes mathématiques complexes et longs à résoudre sans les bonnes informations (clés), malheureusement sans garantie d'inviolabilité. Car il existe une course entre la puissance de calculs des ordinateurs et les algorithmes toujours plus rapides et performants.

Dans le domaine de la communication, la cryptographie classique repose principalement sur 2 méthodes : les clés privées et les clés publiques.

Dans le cas des clés privées, imaginons que pour sécuriser une transmission, Bob et Alice partagent une même clé privée, une suite binaire connue uniquement d'eux. Pour crypter un message (binaire), Bob effectue l'opération $\oplus$ entre son message et sa clé. Pour le décrypter, Alice fera la même opération. Par exemple :

Cryptage de Bob :

Message initial	1	1	0	1	0	0	1	0	1	0
Clé privée	0	1	1	0	1	0	1	1	0	1
Message envoyé	1	0	1	1	1	0	0	1	1	1

Décryptage d'Alice :

Message reçu	1	0	1	1	1	0	0	1	1	1
Clé privée	0	1	1	0	1	0	1	1	0	1
Message Alice	1	1	0	1	0	0	1	0	1	0

$\Rightarrow$ Les 2 messages sont bien identiques.

Pour éviter, qu'une personne qui intercepte le message ne puisse le décoder, il est préférable d'avoir une clé au moins égale au message, et de changer de clé pour chaque message.

Le problème de cette méthode dans le cas classique est la transmission de ces clés. En effet, comment les transmettre de façon sécurisée ? Bob et Alice peuvent se les transmettre en direct, par message, par téléphone... mais ils sont obligés de se transmettre en clair. Or si la clé est interceptée, le cryptage est inutile. Et ce procédé doit être réitéré (de préférence) à chaque message. La transmission de cette clé rend donc difficile la sécurisation des communications par clé privée.

Afin de résoudre ce problème, on utilise l'intrication quantique de 2 particules subatomiques qui serviront de clé. C'est ce qu'on appelle une transmission QKP pour Quantum Key Distribution.

Si Bob envoie à Alice la seconde particule d'un système intriqué (photons de lumière polarisée), une fois qu'Alice l'a reçu, si le système a toujours un état indéterminé alors Bob peut effectuer des mesures sur le système pour crypter son message et lui envoyer, sinon il recommence. Dès qu'Alice reçoit le message, elle peut le décoder avec la certitude que personne d'autre ne pourra le lire.

Donc l'intrication et la superposition quantique pourrait en rendre la communication par clé privée sûre et sécurisée.

Il existe déjà des sociétés qui commercialisent ce genre de solution, mais avec une portée d'une centaine de kilomètres.

2.3 Algorithmes et Complexités

En passant des bits aux qubits, nous devons complètement changer notre façon de penser les algorithmes et les composants électroniques pour prendre en considération leurs propriétés de superposition d'états et d'intrication entre qubits. C'est tout le domaine de l'informatique doit être complètement repensé.

2.3.1 Opérations élémentaires sur les qubits

Les opérations sur des bits se font par l'intermédiaire de portes logiques avec des opérations basiques.

Dans le cas classique, il existe 3 opérations logiques élémentaires : la conjonction $\wedge$ (correspondant au connecteur logique AND/ET), la disjonction $\vee$ (OR/OU), la négation $\neg$(NAN/NON).

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

FIGURE 2.2 – L'opération AND

x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1

FIGURE 2.3 – L'opération OR

x	$\neg x$
0	1
1	0

FIGURE 2.4 – L'opération NEG

À partir de ces 3 opérations, on peut effectuer toutes les opérations sur les bits possibles. Comme le ou exclusif $\oplus$ (XOR) :

$$x \oplus y = (x \vee y) \wedge \neg(x \wedge y)$$

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

FIGURE 2.5 – L'opération XOR

Mais pour que ces opérations fonctionnent (expérimentalement), il faut introduire une autre opération : la copie, telle que :

$$COPY\, x = xx$$

FIGURE 2.6 – L'opération COPY

Ces opérations sont exécutées par des dispositifs numériques. En les accumulant, on construit des ensembles plus complexes comme des additionneurs, qui effectuent la somme mathématique sur nombres entiers (binaires).

L'informatique classique repose entièrement sur ces 4 portes élémentaires. Grâce à elles, on peut construire n'importe quel algorithme ou programme classique.

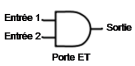

FIGURE 2.7 – La porte ET

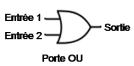

FIGURE 2.8 – La porte OU

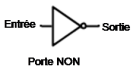

FIGURE 2.9 – La porte NON

Dans le cas quantique, on ne peut pas utiliser les mêmes portes. Par exemple, on a vu précédemment qu'on ne pouvait pas reproduire fidèlement 2 qubits, donc l'opération de $COPY$ n'est pas réutilisable. Il faut trouver des outils capables de manipuler la fonction d'onde des qubits.

Commençons avec la **porte X**, elle a un comportement analogue à la porte NON, c'est-à-dire qu'elle transforme un état $|0\rangle$ en un état $|1\rangle$ et réciproquement :

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

Ensuite la **porte d'Hadamard H**, elle donne une polarisation à 45° :

$$\begin{array}{l} H|0\rangle = |+\rangle \\ H|1\rangle = |-\rangle \end{array} \quad \text{Avec} \quad \left| \begin{array}{l} |+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) \end{array} \right.$$

Si on applique cette porte au vecteur :

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

On obtient alors :

$$\frac{\sqrt{2}}{2}\left[(\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle\right] = \alpha|+\rangle + \beta|-\rangle$$

Avant la transformation, la mesure avait une probabilité de $|\alpha|^2$ de donner $|0\rangle$ et de $|\beta|^2$ de donner $|1\rangle$. Après la transformation, la mesure a une probabilité de $|\alpha|^2$ de donner $|+\rangle$ et de $|\beta|^2$ de donner $|-\rangle$.

La **porte cNOT** (pour *controlled-NOT*) est, quand à elle une porte à 2 qubits :

$$cNOT(|x\rangle|y\rangle) = |x\rangle|x \oplus y)\rangle$$

$|x\rangle$ est un qubit de contrôle, c'est-à-dire que lorsqu'il est dans l'état $|0\rangle$ on ne fait rien, s'il est dans l'état $|1\rangle$ on modifie $|y\rangle$ qui est un qubit cible [5].

Dans un circuit, elles sont représentées par les portes suivantes :

FIGURE 2.10 – La porte X

FIGURE 2.11 – La porte H

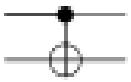

FIGURE 2.12 – La porte cNON

2.3.2 Algorithmes

En modifiant les portes quantiques, on doit à présent changer toute la manière de penser les programmes. Ainsi les algorithmes doivent être réécris et redémontrés. C'est pourquoi les mathématiciens et les informaticiens travaillent sur de nombreux algorithmes qui prennent en compte la superposition et l'intrication quantique.

Aujourd'hui il en existe de plus en plus, et pour illustrer le fonctionnement et l'intérêt de ce genre d'algorithme, on va expliquer l'un des plus connus : l'algorithme de Grover. Son but est de chercher des informations dans une base de données non triées.

Dans le cas classique, on regarde élément par élément jusqu'à trouver le bon. Si on a une base de données à N éléments, alors il faudra effectuer en moyenne $\frac{N}{2}$ tests afin de trouver le bon. Sa complexité est donc linéaire et donc pas très performante. Par exemple, dans le cas d'une base non triée, la recherche est logarithmique (algorithme de recherche par dichotomie).

Avec l'algorithme de Grover la complexité de recherche est $\frac{\pi}{4}\sqrt{N}$. Ainsi pour une base de 10 000 éléments, on passe de 5 000 tests à environ 80 [2].

On note q la valeur que nous cherchons et $f(x) = \delta_{xq}$. Le but de cet algorithme est de trouver x tel que $f(x) = 1$. Pour cela, on utilise un opérateur appelé **Oracle**, défini par :

$$U_f(|x\rangle|-\rangle) = |x\rangle|-\oplus f(x)\rangle$$

On rappelle que $|-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$.

Mais l'oracle ne change pas l'état de $|-\rangle$, par contre il change le signe de $|x\rangle$. On peut donc résumer cette fonction par :

$$U_q(|x\rangle) = (-1)^{f(x)}|x\rangle$$

On note n le nombre de qubits que nous allons utiliser, nous avons donc $N = 2^n$ entrées différentes possibles.

Avant d'effectuer l'algorithme, nous effectuons une mise à zéro de tous les qubits. Notre système est donc dans l'état suivant :

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{x=2^n-1} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{x=N-1} |x\rangle$$

Or même si on ne connait pas encore q, on sait que :

$$|\langle q|\phi\rangle| = \frac{1}{\sqrt{N}}$$

Donc la probabilité de mesure q est de $\frac{1}{N}$. Il faut maintenant augmenter l'amplitude de probabilité de l'état $|q\rangle$. Pour cela, on doit définir un nouvel opérateur G :

$$G = U_\phi U_q$$

Où U_ϕ est une transformation définie par :

$$U_\phi = 2|\phi\rangle\langle\phi| - I$$

Il est invariant pour l'état $|\phi\rangle$ mais il change le signe de tous les opérateurs perpendiculaires.

Ainsi à chaque fois qu'on applique G, on augmente la probabilité de $|q\rangle$ jusqu'à obtenir une probabilité avoisinant 1.

La complexité moyenne de cet algorithme est de : $\frac{\pi}{4}\sqrt{4}$

2.3.3 Problème pour la sécurité numérique

En 1976, Whitfield Diffie et Martin Hellman (Université Stanford) publient un nouveau mode de cryptographie asymétrique, appelé usuellement clé publique. Il s'agit de la cryptographie la plus courante actuellement. Imaginons que Bob cherche à transmettre à Alice un message, et personne ne doit pouvoir le lire même si le message est intercepté.

Ce chiffrement se base sur un remarque simple : il est très facile de multiplier 2 nombres très long et de faire la décomposition en facteur premier d'un nombre. Prenons un nombre $N = pq$, si N et donc p et q sont grands (plusieurs centaines de chiffres) alors faire le produit pq reste simple mais la décomposition en facteurs premiers devient ridiculement long (en mois ou années actuellement). Et ce malgré des siècles à la recherche d'une méthode efficace. Jusqu'aux développements d'algorithmes quantiques, et de l'algorithme de Shor.

Dans le cadre de la cryptographie RSA (du nom de ses 3 concepteurs Rivest, Shamir et Adlema), on utilise des nombres p et q entiers naturels (pour augmenter la complexité du déchiffrement), ce qui nous offre une complexité de $(log(N))^3$. Alors qu'avec l'algorithme de Shor qui utilise le principe d'intrication, la complexité descend à $(ln(N))^3 ln(ln(N)|ln(\varepsilon)|$ [6].

Ce gain de performance, pour casser le chiffrement asymétrique, est l'un des principaux moteurs, pour la recherche de l'information quantique. Il s'agit d'une inquiétude grandissante à cause des avancées fulgurantes dans ce domaine ces dernières années. Car le premier qui parviendra à développer la technologie pour exécuter l'algorithme de Shor, aura un (quasi) libre accès au monde numérique : vies privées, services bancaires, services informatiques quelconques. Puisque la quasi totalité du chiffrement est basée sur RSA. C'est pourquoi de plus en plus d'entreprises et d'institutions gouvernementales [7] investissent dans ce domaine, pouvoir espionner ses alliés et ses ennemis facilement, en étant sûr que personne ne puisse nous espionner. C'est le rêve de tous les pays depuis la Rome Antique et Jules César.

Chapitre 3

L'ordinateur Quantique

3.1 Physique des matériaux

Il existe 3 principaux types de qubits induis par les 3 types de particules utilisées pour les concrétiser : photon, électron ou proton. Ils sont interprétés par propagation de la lumière, par le spin des électrons, le spin nucléaire, ou par le niveau d'énergie (fondamental ou excité). Chacune représente un domaine de recherche complet, mais doivent rester compatibles et complémentaires.

3.1.1 Support élémentaire du qubit

On a vu précédemment qu'un qubit $|\phi\rangle$ possède 3 états différents : $|0\rangle$, $|1\rangle$, ou une combinaison linaire des deux $\alpha|0\rangle + \beta|1\rangle$. À présent nous allons voir comment ils sont matérialisés.

La première méthode est appelée **pont quantique**. Elle consiste à enfermer un électron dans une cage d'atomes, et de le manipuler par des impulsions lasers afin de modifier son niveau d'énergie pour le faire passer d'un état fondamental à excité, ou réciproquement. Le niveau d'énergie du laser ainsi que la durée d'exposition de l'électron sont parfaitement définis. Ainsi pour obtenir la superposition quantique, il faut lui appliquer un signal moitié moins long que celui qui le fait changer de niveau d'énergie. Mais cet état n'est pas stable, l'électron ne reste pas indéfiniment dans cet « entre 2 » états, ce qui provoque de la décohérence[8].

La second méthode utilise le spin nucléaire des protons d'une molécules, appelée **RMN** pour **résonance magnétique nucléaire**. La RMN est la manipulation du spin par des impulsions radio-fréquences. Cette méthode est moins sujette aux erreurs car si la molécule change d'état d'énergie ses valeurs de spin ne sont pas modifiées, ce qui ralentit l'apparition du phénomène de décohérence[8].

En 2001 Chuang d'IBM, est parvenu à exécuter l'algorithme de Shor sur une molécule avec 7 spins nucléaires, et il est parvenu à factoriser le nombre 15. Il a ainsi montré expérimentalement la faisabilité de l'algorithme.

Le problème de cette méthode, en plus de la décohérence, est la limite du nombre de qubits. On ne peut pas travailler avec une centaine ou un millier de qubits, car on est limité par la taille des molécules et par l'intensité de leurs champs magnétiques qui est divisée par 2 à chaque fois que l'on ajoute 1 seul qubit.

Mais un ordinateur quantique ne doit pas uniquement effectuer des calculs mais aussi communiquer et stocker de l'information.

Pour communiquer on privilégiera la **polarisation de la lumière**. On considère qu'une polarisation horizontale correspond à un état $|0\rangle$, une polarisation verticale à l'état $|1\rangle$ et tous les autres états intermédiaires correspondront à la combinaison linéaire des 2.

Cette méthode est privilégiée dans la communication car le photon n'a pas de masse et par conséquent il se déplace plus vite que n'importe quelle autre particule. De plus, nous avons vu précédemment que la communication quantique existe déjà (clé privée), mais elle est confrontée à des problèmes pour maintenir sa cohérence. Car même si la planète est déjà connectée par des fibres optiques, les câbles utilisés ne sont pas parfaits, ce qui provoque du bruit qui augmente avec le carré de la distance. Dans le cas classique, il existe des méthodes pour amplifier les ondes. Mais dans le cas quantique on ne peut pas les utiliser sans provoquer encore plus de décohérence et anéantir notre superposition.

Pour stocker des informations, on peut utiliser des **pièges à ions**. Il s'agit de créer un nuage de particules qui va interagir avec le photon qui porte l'information à conserver. Sous l'effet d'un laser le nuage laisse entrer le photon, et lorsqu'on éteint le laser, le photon reste piégé dans le nuage, jusqu'à ce qu'on rallume le laser.

3.1.2 Recherches : collaboration entre les universités de Strasbourg et de Rouen

L'université de Strasbourg cherche à concevoir un matériau qui servirait de support aux qubits. Ce qubit serait une nanoparticule, constituée de ZnO et de Manganèse dans un substrat d'alumine (isolant). Ce qui permettrait d'allier les propriétés du supraconducteur ZnO et les propriétés magnétiques du spin nucléaire du Manganèse.

Actuellement Amjad Abou Latif du GPM étudie un premier échantillon grâce à la sonde atomique afin de déterminer son organisation atomique. L'objectif est de réaliser des nanoparticules de ZnO, sans le Manganèse dans un substrat d'alumine. Malheureusement, les résultats montrent que dans l'échantillon les molécules de Zn0 ne forment pas de nanoparticules mais une couche.

Dans un second échantillon le substrat d'alumine a été remplacé par un substrat de Silice. Dans l'attente de l'expérience sur la sonde atomique, il a été observé au microscope électronique à balayage. Cette fois on observe bien des nanoparticules mais pour l'instant on ne connait pas encore les constituants atomiques avec précision.

Image TEM : HAADF (High Angle Annular Dark Field)

Al_2O_3 implanté Zn^{66}

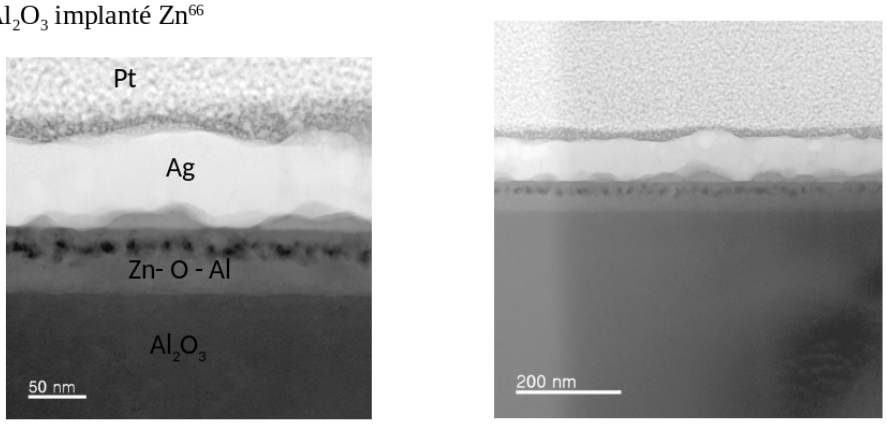

FIGURE 3.1 – Le 1er échantillon : on voit une couche de Zn avec des petits trous.

Image MEB : SiO_2 implanté Zn^{66}

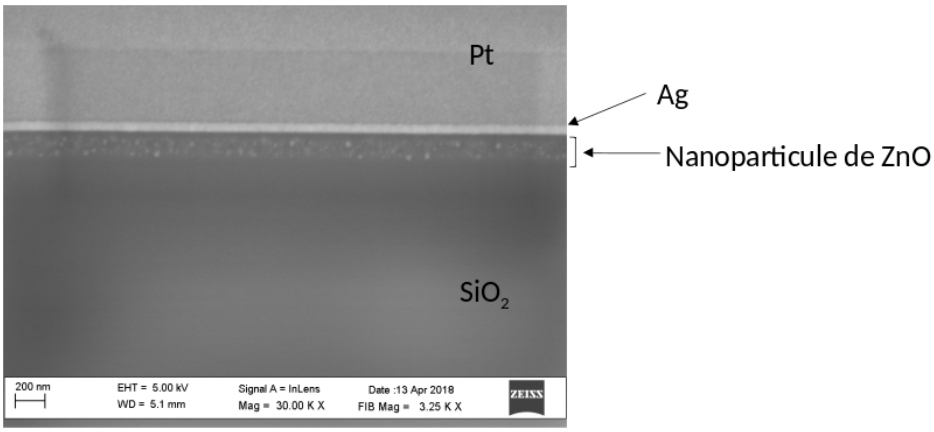

FIGURE 3.2 – Le 2nd échantillon : cette fois on peut observer des nanoparticules de Zn0.

3.1.3 Les calculateurs quantiques

L'objectif des scientifiques dans ce domaine n'est pas de créer une nouvelle technologie capable de remplacer nos outils technologiques personnels. On parle de technologie hybride, car en dehors de la sécurisation de nos données privées, où quelques qubits assureraient la sûreté de nos données et de nos communications, la technologie classique actuelle est suffisante (et même supérieure). Les chercheurs veulent mettre au point un nouveau type de calculateur, d'une puissance de calculs très supérieure, grâce aux propriétés quantiques.

Avant de commencer, faisons une mise au point du vocabulaire. Un **calculateur quantique** effectue des calculs en utilisant les propriétés quantiques d'intrication, de superposition, entre autres. Alors qu'un **ordinateur quantique** est capable, en plus, de stocker de l'information et de communiquer sur le réseaux. Ainsi l'ordinateur quantique n'est pas encore d'actualité, mais les avancés en matière de calculateur sont très prometteuses.

Plusieurs entreprises sont lancées dans la R&D de l'ordinateur quantique, avec parfois très approches des différentes. Plusieurs calculateurs quantiques existent déjà et sont même commercialisés.

En 2011, l'entreprise **DWave System** commercialise, ce qu'ils présentent comme le premier ordinateur quantique à 128 qubits, *D-WAVE*. Depuis elle a commercialisé le *D-WAVE TWO* à 512 qubits en 2013, et aujourd'hui elle a dépassé les 2 000 qubits pour 15 millions de dollars. Malheureusement, de l'extérieur nous ne pouvons pas en juger, car la machine est protégée par des brevets et le secret industriel. Cependant des experts indépendants accrédités par l'entreprise, assurent que ce n'est pas un ordinateur quantique, les qubits n'ont pas une qualité suffisante pour pouvoir exécuter des algorithmes quantiques. Il s'agirait plutôt d'un **optimisateur quantique**, c'est-à-dire qu'il utilise des effets quantiques (comme l'effet tunnel) pour améliorer la résolution de problèmes numériques. Sans information supplémentaire, la communauté scientifique ne peut pas trancher, mais elle reste perplexe sur la faisabilité d'un calculateur quantique, surtout composé d'autant de qubits.

Il existe un processeur quantique de **5 qubits** fonctionnant grâce à la technologie des **supra-conducteurs**. Malheureusement pour lutter contre la décohérence quantique, sa température doit être maintenue à $-273°C$.

Mais cette puce quantique a été mise à disposition des internautes via une plateforme de *cloud computing* du nom de « IBM Quantum Experience ». Il suffit de faire une demande et de justifier de son niveau dans le domaine et gratuitement des entreprises, des laboratoires, des étudiants ou des personnes lamdas peuvent effectuer des simulations sur ce processeur à l'aide de vrais qubits. [9]

Cette initiative cherche à promouvoir cette technologie, et à la rendre accessible à plus de monde, afin de développer l'intérêt et le R&D. Car d'après IBM, les premiers calculateurs à 50-100 qubits devraient voir le jour dans les 10 ans à venir. [10]

Et cette initiative fonctionne, en moins d'un an il y a eu 275 000 requêtes pour 40 000 personnes, dont 15 chercheurs ont publié des articles en utilisant ou citant ce processeur [11].

Des scientifiques sont parvenus à construire à partir d'une **puce de Silicium** de microprocesseur classique en quantique, ce qui permet de s'affranchir de la supraconductivité (et de pouvoir élever un peu la température). Il s'agit de qubits spin, c'est-à-dire d'électrons exités par des ondes électro-magnétiques [12]. Grâce à cette méthode, les qubits sont plus stables, car ils sont moins influençables par les ondes EM, ils peuvent être utilisés à des températures supérieures qu'avec la méthode des supra-conducteurs et donc on réduit considérablement la taille des dispositifs de maintien des températures (Intel QuTech).

Récemment, Intel a partagé une pouce de **17 qubits** avec QuTech pour qu'il puisse effectuer des tests face à l'exécution de programme. Intel prétend que leur nouvelle puce serait plus fiable, moins fragile face aux interférences radio-fréquences et s'échaufferait moins. Mais cette pouce est à usage interne et ne pourra par être tester par la communauté scientifique. [13]

Cependant nous ne pouvons pas garantir l'avancée de cette technologie, car pour des raisons de confidentialité une partie de cette recherche est divulguée voir dissimulée au public.

Ainsi des rumeurs courent concernant l'entreprise chinoise Huawei et des agences gouvernementales américaines, principalement la NSA, qui développerait cette technologie depuis des années. Mais pour des raisons de sécurité ou de concurrence, ils préfèrent dissimuler leurs recherches et leurs avancées.

Dans tous les cas l'objectif prioritaire de tous les constructeurs de calculateur quantique est d'atteindre les 50 qubits. Cela parait peu, surtout quand on compare aux nombres de bits classiques de nos outils quotidiens, mais c'est suffisant pour rendre obsolète les super-ordinateurs actuels, et casser l'ensemble des systèmes de cryptographie. [10] C'est ce qui est appelé la **suprématie quantique**. En sachant que le calculateur qui atteindra les 100 qubits surpassera la puissance totale de tous les super-ordinateurs du monde combinés.

Mais avant la suprématie quantique, il faut apprendre à augmenter le nombre de qubits. En effet, pour maintenir la cohérence d'un qubit, il faut des conditions extrêmes, puisqu'il faut le maintenir dans un environ-

FIGURE 3.3 – Le D-WAVE de DWAVE System

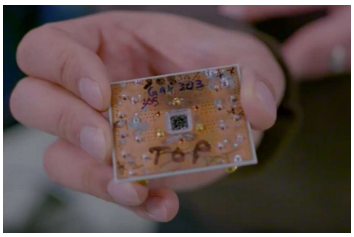

FIGURE 3.4 – La puce à 5 qubits d'IBM au centre du circuit imprimé

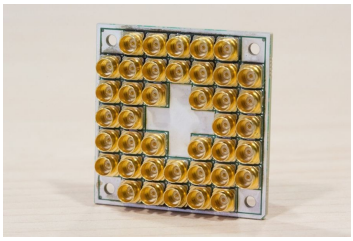

FIGURE 3.5 – Une des puces en Silicium d'Intel-QuTech

nement isolé proche de 0K. Sauf qu'avec un seul qubit les calculs sont très limités, on a besoin de multiplier ce nombre. Mais les qubits interagissent entre eux, ce qui provoque aussi la perte de la superposition d'états, donc de l'information. Le maintien de la cohérence quantique représente le principal obstacle à l'augmentation du nombre de qubits. De plus, avec l'augmentation des qubits, il faut parvenir à les identifier et les manipuler séparément, et donc avec des outils et techniques très précises.

Des correcteurs peuvent être mis en place mais pour qu'ils soient efficaces, des scientifiques ont prouvé que le nombre d'erreurs ne devait pas dépasser une pour 10 mille opérations. [14]

C'est pourquoi certains misent sur l'ordinateur quantique topologique [15]. Pour s'affranchir de la décohérence, il utilise la théorie des tresses mathématiques et l'effet Hall quantique. À la place de regarder l'état des particules, on analyse leurs trajectoires les unes par rapport aux autres, ce qui permet de réduire la décohérence.

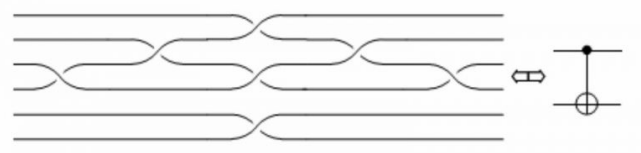

FIGURE 3.6 – Analogie entre la porte quantique cNOT et l'équivalent « topologique » (*Démontré en 2005 par Nicholas Bonesteel*). Ce schéma représente 6 trajectoires (ou **lignes d'univers**) de 6 qubits (**des fermions de Majorana**).

Mais là où les choses se compliquent c'est qu'on a besoin d'utiliser les **fermions de Majorana**. Ces pseudo-particules ont juste une masse, elles n'ont ni énergie, ni charge électrique, et surtout elles sont leurs propres antiparticules. C'est pourquoi cette particule est très difficile à détecter expérimentalement car la seule façon de la détecter c'est sa masse (c'est pourquoi, il s'agit de la meilleure candidate pour la matière noire).

Ainsi l'ordinateur topologique mise sur les mathématiques et la physique subatomique théorique pour concevoir son ordinateur. Il s'agit d'une entreprise risquée, mais si cela fonctionne la multiplication du nombre de qubits sera « plus facile » que pour les autres technologies. Cependant les premiers qubits seront beaucoup plus compliqués à mettre en place.

Pour comparer les différents ordinateurs quantiques, on peut calculer le nombre n d'opérations qu'il pourra effectuer avant de perdre leur cohérence. Il s'agit du rapport entre le temps T où le système reste quantique et le temps mis par une porte logique pour modifier un qubit :

$$n = \frac{T}{t}$$

n : nombre d'opérations effectuées avant décohérence
T : temps de cohérence de l'ordinateur
t : temps pour effectuer une opération

On remarque que la durée d'utilisation de l'ordinateur topologique est plus longue et quelle génère moins d'erreurs. Mais les autres technologies ont déjà des applications.

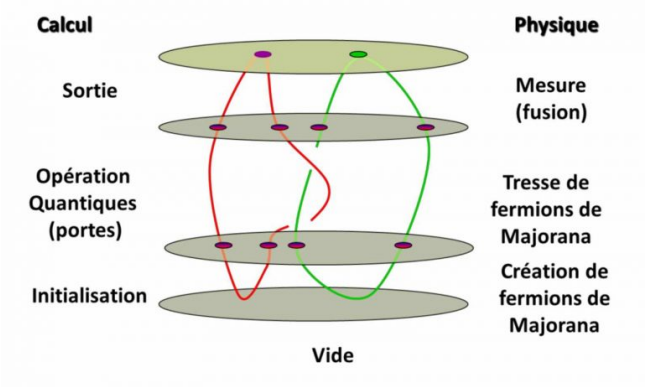

FIGURE 3.7 – Fonctionnement d'un ordinateur topologique[14] - *Création à partir du vide de 2 fermions de Majorana, exécution de l'algorithme (opérations quantiques ou tresses de fermions), et la mesure (observation de la fusion des fermions).*

Technologies	Durée de vie	Vitesse de la porte	Coût de la correction d'erreur
Topologique (Majorana)	**1 minute**	**Nanosecondes**	**10^1**
Flux Qubit	/ 10^{10}	Idem	$10^3 - 10^4$
Charge Qubit	/ 10^{10}	Idem	$10^3 - 10^4$
Transmon	/ 10^7	Idem	$10^3 - 10^4$
Piège à ion	/ 10^2	10^3 plus lent	$10^3 - 10^4$

FIGURE 3.8 – Comparaison des différentes technologies en développement [14]

3.2 Simulation quantique

La simulation quantique s'effectue sur un super-ordinateur classique qui reproduit le raisonnement qu'aurait un calculateur quantique. Il s'agit de super-ordinateurs qui simulent des embryons de calculateurs quantiques.

Ce type de simulation permet d'avancer dans le domaine de la chimie, de la physique des particules, de la physique des matériaux... Elle est utilisée pour concevoir des molécules ou des matériaux qui n'existent pas (encore), ou qui sont très compliqués à observer [16].

En effet, les ordinateurs classiques sont vite dépassés par le nombre de paramètres à prendre un considération dans certaines simulations, surtout quand elles doivent prendre en compte plusieurs notions de physique complexe. Par exemple, un ordinateur classique ne peut pas simuler l'entrée atmosphérique d'engins spatiaux, car il doit manipuler 3 physiques différentes : la mécanique des fluides pour les particules de l'atmosphère, la physique des plasmas pour l'échauffement de l'engin et la chimie pour les réactions entre le milieu et l'engin. Par contre un simulateur classique arrive parfaitement à manipuler le vol d'un avion qui a principalement besoin de la mécanique des fluides.

Avec les simulateurs quantiques, on pourrait augmenter la difficulté des problèmes solubles par simulation numérique. Notamment dans le domaine de la physique des matériaux, où les simulations quantiques aident déjà à mieux comprendre leur fonctionnement [17]. Ainsi en modifiant légèrement certains paramètres comme la distance entre les atomes, leurs répartitions, la densité des espèces chimiques... les scientifiques peuvent déterminer quelles sont les meilleurs combinaisons à utiliser pour la concevoir de nouveaux matériaux qui répondront au mieux aux caractéristiques posées, et cela avant même de construire le moindre dispositif. Cette méthode a déjà fait ses preuves dans l'aéronautique et l'aérospatiale et leur permet de limiter le nombre de prototypes, d'accélérer la R&D et donc de réduire le coût.

Mais le principal avantage de concevoir ce type de simulateur est qu'il ne subit pas de décohérence, puisqu'il est classique.

En attendant d'être capable de construire un calculateur quantique, certaines entreprises construisent donc des ordinateurs classiques capables d'imiter quelques qubits. Il s'agit de super-ordinateur destiner aux laboratoires et entreprises qui souhaitent mettre en pratique leurs algorithmes, et effectuer des calculs quantiques.

Ainsi depuis juillet 2017, l'entreprise **Atos** commercialise un supercalculateur capable de reproduire un ordinateur de 30 à 40 qubits (pour 100 mille à 1 millions d'euros), nommé **QLM** pour « **Quantum Learning**

Machine » [18, 19]. Il s'agit d'un appareil de transition qui permet de tester les algorithmes et programmes quantiques afin de développer l'information quantique en attendant que la technologie des 1ers ordinateurs quantiques soit prêtes.

L'entreprise a 3 objectifs : le développement d'algorithmes quantiques, ainsi que des systèmes capables de résister à des attaques quantiques et d'accompagner la recherche sur l'information quantique.

Avec le QLM, Atos cherche aussi à développer la programmation quantique. C'est pourquoi au même moment, Atos lance un nouveau langage de programmation, **aQasm** pour **Atos quantum assembly langage**, compatible avec les environnements déjà existant de Google et Microsoft, Playground et Liquid.

Car, même si la technologie n'est pas prête sont objectifs final reste d'exécuter des algorithmes, donc il faut que les développeurs commencent à s'impliquer pour construire avec les ingénieurs et les chercheurs afin que le produit soit performant à l'utilisation.

Chapitre 4

Conclusion

Avec la fin de la loi de Moore, on peut se demander quel sera l'avenir et les évolutions de l'informatique. Pour le forger, de plus en plus d'entreprises et d'États misent et investissent sur la physique quantique.

En effet aujourd'hui ils sont capables de concevoir les premiers calculateurs quantiques, les premiers systèmes de communication sécurisés grâce à la superposition d'états et à l'intrication quantique. Et les entreprises et laboratoires spécialisés nous promettent la suprématie quantique dans la décennie à venir.

Cependant la recherche sur l'information quantique est encore à ses débuts. Nous sommes très loin d'un ordinateur quantique autonome et fonctionnel. Dans les prochaines années, on imagine plutôt des systèmes duals, où la physique quantique viendrait corriger ou améliorer des points défaillants de notre système actuel, pour la sécurisation ou l'amélioration de l'accès aux données et de nos communications. Et où des calculateurs quantiques effectueraient les calculs et les simulations trop complexes pour les super-calculateurs dits classiques.

Mais l'engouement actuel pour l'ordinateur quantique nous promet de belles surprises. Car les scientifiques, artistes, politiques ne sont jamais parvenus à anticiper les mutations des prochaines décennies et encore moins le destin de leurs propres recherches. Qui aurait pu prédire il y a un siècle que la recherche fondamentale sur la nature de la lumière à l'origine de la physique quantique amènerait à la numérisation et au changement complet qu'elle a eu sur notre société. Personne ne peut savoir quand et comment l'information quantique aboutira, ni même si elle aboutira.

Vus d'artistes de 1899 de l'an 2000, exposés lors de l'exposition universelle de 1900 à Paris

Annexe A

Rappels Physique

A.1 Principe de Pauli

Définition : Les **Fermions** regroupent les particules qui ont un spin non entier, comme les électrons qui possèdent un spin $\frac{1}{2}$. En opposition, aux **Bosons** de spin entier, comme les photons de spin 1.

Principe d'exclusion de Pauli : Dans un système de fermions, on ne peut pas avoir 2 fermions dans le même état quantique au même endroit.

A.2 L'effet Tunnel

Découvert en 1928 par Geaorges Gamov, l'effet tunnel est purement quantique.

Si on envoie un ballon contre un mur, il rebondit. De même si on envoie des particules, sauf si le mur est suffisamment fin. Les particules quantiques se comportant à la fois comme des particules et des ondes, certaines particules pourraient traverser le mur comme des ondes. Et plus le mur est fin plus la probabilité d'avoir des particules qui traversent le mur augmente.

En effet, si l'énergie potentielle d'une particule est supérieure à son énergie cinétique, la particule classique rebondit, alors que la particule quantique aurau unne probabilité non nulle de franchir l'obstacle.

Annexe B

Démonstration de l'inégalité de Bell

On se place dans la théorie réaliste locale EPR. En un instant, et en un endroit donnés, on désintègre une particule de spin 0, ce qui émet une paire de particules intriquées, électron-positron, dans 2 directions opposées, vers 2 opérateurs, Alice et Bob. On not A l'électron reçu par Alice et B le positron de Bob. Donc, il existe 2 configurations possibles : soit l'électron a un spin up $+1/2$ et le positron un spin down $-1/2$, soit l'électron a un spin down $-1/2$ et le positron un spin up $+1/2$.

Alice et Bob vont effectuer des mesures de spin selon la direction du vecteur de Bloch $\vec{n}$ avec :

$$\begin{cases} n_x = \sin\theta\cos\phi \\ n_y = \sin\theta\sin\phi \\ n_z = \cos\theta \end{cases} \tag{B.1}$$

On se fixe 3 vecteurs $\vec{n}_1$, $\vec{n}_2$ et $\vec{n}_3$, et on effectue une mesure par axe pour chaque particule reçue. Chaque mesure pouvant donner 2 résultats différents, on a 2^3 situations différentes :

	Alice			Bob		
	$\vec{n}_1$	$\vec{n}_2$	$\vec{n}_3$	$\vec{n}_1$	$\vec{n}_2$	$\vec{n}_3$
N_1	+1	+1	+1	-1	-1	-1
N_2	+1	+1	-1	-1	-1	+1
N_3	+1	-1	+1	-1	+1	-1
N_4	+1	-1	-1	-1	+1	+1
N_5	-1	+1	+1	+1	-1	-1
N_6	-1	+1	-1	+1	-1	+1
N_7	-1	-1	+1	+1	+1	-1
N_8	-1	-1	-1	+1	+1	+1

FIGURE B.1 – Toutes les possibilités de résultats de mesures des spin

On remarque que pour les cas 3 et 4, suivant l'axe $\vec{n}_1$ pour Alice et $\vec{n}_2$ pour Bob leurs résultats sont identiques. Prenons certains cas du tableau précédent et regroupons les :

	Alice			Bob		
	$\vec{n}_1$	$\vec{n}_2$	$\vec{n}_3$	$\vec{n}_1$	$\vec{n}_2$	$\vec{n}_3$
N_3 et N_4	+1				+1	
N_2 et N_4	+1					+1
N_3 et N_7			+1		+1	

FIGURE B.2 – Tableau réduit avec des résultats identiques pour Alice et Bob

Donc la probabilité d'être dans le cas où Alice est $+1$ suivant $\vec{n}_1$ (resp. $\vec{n}_1$ et $\vec{n}_3$) et Bob $+1$ suivant $\vec{n_2}$ (resp. $\vec{n}_3$ et $\vec{n}_2$) est :

$$P_{\vec{n}_1\vec{n}_2}(+1) = \frac{N_3 + N_4}{N}$$

$$P_{\vec{n}_1\vec{n}_3}(+1) = \frac{N_2 + N_4}{N}$$

$$P_{\vec{n}_3\vec{n}_2}(+1) = \frac{N_3 + N_7}{N}$$

Or si on additionne les probabilités de $P_{\vec{n}_1\vec{n}_3}(+1)$ et $P_{\vec{n}_3\vec{n}_2}(+1)$:

$$P_{\vec{n}_1\vec{n}_3}(+1) + P_{\vec{n}_3\vec{n}_2}(+1) = \frac{N_2 + N_4}{N} + \frac{N_3 + N_7}{N}$$

Et comme $n_1 \leqslant n_1 + n_2,\ \forall n_1, n_2$ réels positifs, est toujours vrai. On peut dire que :

$$\frac{N_3 + N_4}{N} \leqslant \frac{N_2 + N_4}{N} + \frac{N_3 + N_7}{N} \leqslant 1$$

$$P_{\vec{n}_1\vec{n}_2}(+1) \leqslant P_{\vec{n}_1\vec{n}_3}(+1) + P_{\vec{n}_3\vec{n}_2}(+1) \leqslant 1$$

Cette inégalité est toujours vraie, sinon c'est que notre hypothèse est fausse, celle de la théorie réaliste locale EPR.

Lorsque l'on projette la mesure de spin suivant les 3 directions de $\vec{n}$, on obtient :

$$\vec{\sigma}.\vec{n} = n_x\sigma_1 + n_y\sigma_2 + n_z\sigma_3$$

Or on admettra que $\vec{\sigma}.\vec{n}$ a pour vecteur propre :

$$|\phi_+\rangle = \cos\tfrac{\theta}{2}|+\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|-\rangle$$
$$|\phi_-\rangle = -e^{-i\varphi}\sin\tfrac{\theta}{2}|+\rangle + \cos\tfrac{\theta}{2}|-\rangle$$

Donc si notre système est dans un état $|\phi_+\rangle$ (resp. $|\phi_-\rangle$), on peut calculer sa probabilité d'être dans un état $|+\rangle$ (resp. $|-\rangle$) :

$$|\langle +|\phi_+\rangle|^2 = \cos^2\frac{\theta}{2}$$
$$|\langle -|\phi_-\rangle|^2 = \sin^2\frac{\theta}{2}$$

Donc l'état intriqué devient :

$$|\beta_{11}\rangle = \frac{\sqrt{2}}{2}(|\phi_+\rangle_A|\phi_-\rangle_B - |\phi_-\rangle_A|\phi_+\rangle_B)$$

Donc la probabilité $P_{\vec{n}_1\vec{n}_2}(+1)$ devient :

$$\begin{aligned} P_{\vec{n}_1\vec{n}_2}(+1) &= |{}_a\langle\phi_+|{}_b\langle\phi_+|\beta_{11}\rangle|^2 \\ &= \frac{1}{2}\left[{}_a\langle\phi_+|\phi_+\rangle_{ab}\langle\phi_+|\phi_-\rangle_a - {}_a\,\langle\phi_+|\phi_-\rangle_{ab}\langle\phi_-|\phi_-\rangle_a\right]^2 \\ &= \frac{1}{2}|{}_b\langle\phi_+|\phi_-\rangle_a|^2 \\ &= \frac{1}{2}\sin^2\frac{\theta_{12}}{2} \end{aligned}$$

Donc la probabilité $P_{\vec{n}_1\vec{n}_3}(+1)$ devient :

$$P_{\vec{n}_1\vec{n}_3}(+1) = \frac{1}{2}\sin^2\frac{\theta_{13}}{2}$$

Donc la probabilité $P_{\vec{n}_3\vec{n}_2}(+1)$ devient :

$$P_{\vec{n}_1\vec{n}_3}(+1) = \frac{1}{2}\sin^2\frac{\theta_{32}}{2}$$

Avec $\left|\begin{array}{l}\theta_{12} = (\vec{n}_1, \vec{n}_2) \\ \theta_{13} = (\vec{n}_1, \vec{n}_3) \\ \theta_{32} = (\vec{n}_3, \vec{n}_2)\end{array}\right.$

Si on reprend l'inégalité précédente, on obtient :

$$\sin^2\frac{\theta_{13}}{2} \leqslant \sin^2\frac{\theta_{13}}{2} + \sin^2\frac{\theta_{32}}{2}$$

Choisissons un cas particulier où : $\theta_{13} = \theta_{32} = \theta$ et $\theta_{ab} = 2\theta$. notre inégalité devient alors :

$$\sin^2\theta \leqslant 2\sin^2\frac{\theta}{2}$$

Or si $0 \leqslant \theta \leqslant \frac{\pi}{2}$ l'inégalité est violée. Donc notre hypothèse de la théorie réaliste locale EPR est fausse. Donc la physique quantique n'est pas déterministe, elle est complète et il n'existe pas de variable cachées.

Annexe C

Compléments sur les ordinateurs topologiques

Mais pour que cette théorie mathématique fonctionne dans le cadre de l'information quantique il faut être dans un espace à 2D, sinon l'application ne serait pas stable (fusion de ligne), donc on a besoin de « particules 2D », les anyons.

Ce sont des quasi-particules dans un espace à 3 dimensions : 2 spatiales et 1 temporelle. Ce ne sont pas des fermions mais elles respectent le principe de Pauli comme les électrons.

Pour le concevoir, on place 2 plaques de semi-conducteur en arséniure de gallium séparées par une fine couche d'électrons libres. Ces 2 couches doivent être suffisamment proches pour que les électrons ne puissent pas se déplacer suivant la normale aux plaques. On applique alors suivant cette même normale, un champ magnétique pour générer un effet Hall classique. Si on augmente le champ et qu'on baisse fortement la température, des paliers d'énergies apparaissent et on parle alors d'effet Hall quantique (Von Klitzong, prix Nobel 1985). Or en 2005 Goldman, Camino et Zhou ont prouvé expérimentalement qu'on obtenait alors des anyons (prix Nobel).

Les permutations entre ces anyons seront les opérations de base pour les qubits, ce qui forme les tresses.

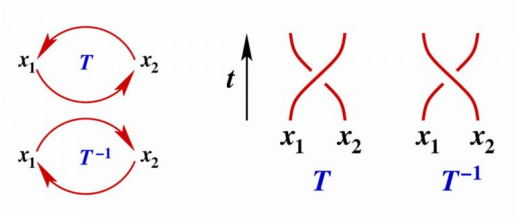

FIGURE C.1 – Création des tresses élémentaires

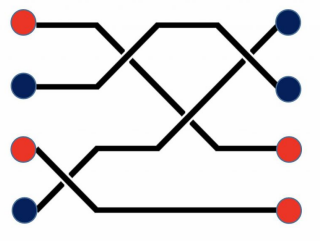

FIGURE C.2 – Exemple de tresses à 2 qubits

La théorie mathématique des tresses forme un groupe non commutatif, ce qui permet de différentier si la rotation est horaire ou trigonométrique.

La permutation de 2 anyons modifie le signe de la fonction d'onde, ce qui permettrait au fil des opérations, de modifier les amplitudes des ondes et de résoudre les algorithmes.

Bibliographie

[1] Laurent Sacco. Loi de moore, feb 2013. https ://www.futura-sciences.com/tech/definitions/informatique-loi-moore-2447/.

[2] Charles Corge. *L'informatique Quantique*. ellipses, 2011.

[3] Eistein, Podolsky, and Rosen. Can quantum-mechanical description of physical reality be considered complete ? 1935.

[4] William Kent Whootters and Wojciech Hubert . A single quantum cannot be cloned. 1982.

[5] Michel Le Bellac. *Le Monde Quantique*. EDP Sciences, 2010.

[6] Nicolas Macris. *Traitement Quantique de l'Information*. PhD thesis, 2014.

[7] Steven Rich and Barton Gellman. Nsa seeks to build quantum computer that could crack most types of encryption, Jan 2014.

[8] Thierry Lombry. *Fabrication d'un ordinateur quantique*. 2015. https ://www.futura-sciences.com/sciences/dossiers/physique-ordinateur-quantique-552/page/6/.

[9] Marc Zaffagni. Testez le processeur quantique d'ibm depuis votre ordinateur !, may 2016.

[10] David Feugey. Ibm met l'ordinateur quantique à la portée de tous, en mode cloud, may 2016. www.silicon.fr.

[11] Sébastien Dumoulin. Ordinateurs quantiques : Ibm veut accélérer, mars 2017.

[12] Rénald Boulestin. Ordinateur quantique : Intel et qutech avancent vers un usage commercial, fev 2018. www.silicon.fr.

[13] Christophe Lagane. Intel avance dans l'informatique quantique avec un premier processeur 17-qubit, oct 2017. www.silicon.fr.

[14] Reynald Fléchaux. Microsoft se lance à son tour dans la course au 1er ordinateur quantique, nov 2016. www.silicon.fr.

[15] Bernard Ourghanlian. Ordinateur quantique : Intel et qutech avancent vers un usage commercial, fev 2018. https ://experiences.microsoft.fr/technique/transform-to-cloud/ordinateur-quantique-topologique/.

[16] Pablo Arrighi and Simon Perdrix. La décohérence, une alliée pour la simulation. *La recherche*, Juillet-Août 2015. Dossier.

[17] Philippe Pajot. Le monde des particules quantiques est subtil et déroutant. *La recherche*, Juillet-Août 2015. Interview Serge Haroche.

[18] Sébastien Dumoulin. Atos dévoile son premier simulateur quantique, jul 2017.

[19] Atos. Atos quantum - une réelle aventure collective, humaine et technologique commence. https ://atos.net/fr/vision-et-innovation/atos-quantum.

[20] Alain Aspect. Experimental test of bell's inequalities using time varying analyzers. 1982.

[21] Elena Castellani, Leonardo Castellani, and Hagen Kleinert. Feynman, génie magicien. *Pour la science*, Mai-Août 2004. Biographie de Feynman.

[22] Philippe Pajot, Gautier Cariou, Eleni Diamanti, and Sébastien Tanzilli. Les révolutions quantiques. *La recherche*, Juillet-Août 2015. Dossier.

[23] Sean Bailly. L'intrication quantique confirmée par une expérience de bell sans faille, Oct 2015. www.pourlascience.fr.

[24] Laurent Sacco. Une mémoire électromécanique pour ordinateur quantique, feb 2013. https ://www.futura-sciences.com/sciences/actualites/physique-memoire-electromecanique-ordinateur-quantique-44705/.

[25] Laurent Sacco. Ordinateur quantique : une nouvelle mémoire avec du diamant, nov 2016. https ://www.futura-sciences.com/sciences/actualites/physique-ordinateur-quantique-nouelle-memoire-diamant-maj-11990/.

[26] Roubert Benoit. *Approche semi-classique de l'information quantique*. PhD thesis, Université de Toulouse, 2010.

[27] Rénald Boulestin. Ordinateur quantique : Intel et qutech avancent vers un usage commercial, fev 2018. www.silicon.fr.

[28] Khalid Latrach. *Introduction à la théorie des points fixes métrique et topologique.* Rérérences sciences, 2017.

[29] Claude Albert. *Topologie.* Edition espace, 1997.

[30] Elisabeth Burroni. *La topologie des espaces métriques.* Ellipses, 2005.