L'informatique quantique : son apport aux processeurs de demain

L'informatique quantique est une technologie du futur, quels bénéfices peut-on en attendre pour les microprocesseurs de demain ?

Mémoire de Recherche pour l'obtention du double diplôme

M2IRT 2011, Master 2 SIC Pro
Systèmes Temps Réels et Communicants

Réalisé par : Jérôme DIAZ
Sous la direction de : Virginie SANS

Promotion 2011

Préambule

Remerciements

Je tiens à remercier tous les intervenants de l'ITIN et de l'Université de Cergy-Pontoise, ainsi que l'intégralité du personnel administratif. La formation qui m'y a été dispensé au cours des cinq dernières années me sera utile pour ma future carrière professionnelle. Il en sera de même de l'expérience que j'ai pu acquérir grâce à l'alternance.

Je pense également aux docteurs Daniel Esteve et Julia Kempe pour avoir accepté de répondre à mes questions et de trouver du temps pour les interviews.

Je n'oublie pas Mlle Virginie Sans, ma directrice de mémoire, que je remercie pour avoir proposé un sujet passionnant faisant appel à la fois à la physique et aux mathématiques. Je la remercie également pour ses retours sur ce document.

J'aimerais aussi adresser mes remerciement à Mme Malika Grim, ma directrice de stage à l'INSERM. Les différents travaux et projets qu'elle m'a confié m'ont permis de m'habituer à la recherche et à la lecture d'articles à caractères scientifiques, notamment en anglais. Elle m'a également autorisé à poser des jours de congés à chaque fois que j'en ai eu besoin pour travailler sur mon mémoire. C'est également lors de mon passage à l'INSERM que j'ai pu me familiariser avec le langage LaTeX, utilisé pour la rédaction de ce document.

Je souhaite finalement remercier ma famille et mes proches pour m'avoir soutenu et encouragé tout au long de mes études.

Abstract

Quantum computing is a new way of designing computers. It uses quantum mechanical phenomena, both at the hardware and software level, to create a computer that can be exponentially faster than a traditional one to perform some tasks. Instead of working with bits, that is to say only with 0 or 1 values, it can also work with a superposed state : 0 and 1 at the same time.

It is known that, in the process of miniaturizing components, will happen a day when we won't be able to ignore quantum phenomena anymore. That is why it is important to work on quantum computing, a new kind of processing that will work behind this wall.

How will this new way of computing affect today's processors ? How to use it to design tomorrows computers ? How will they be built and used ? Those are the questions this research paper will attempt to answer.

Résumé

L'informatique quantique est une autre façon de concevoir les ordinateurs. Elle est basée sur des phénomènes quantiques, utilisés à la fois au niveau matériel et logiciel, et ce pour créer des ordinateurs qui peuvent être exponentiellement plus rapide, sur certaines tâches, que ceux actuels. Plutôt que de travailler sur des bits, c'est-à-dire des valeurs 0 ou 1, elle utilise aussi un état superposé : à la fois 0 et 1.

Nous savons déjà que sur dans la course à la miniaturisation arrivera un jour où il ne sera plus possible d'ignorer les phénomènes quantiques. C'est pour cela qu'il est important de travailler sur l'informatique quantique, une autre façon de calculer qui fonctionne derrière cette barrière.

Comment ce nouveau type d'informatique va influencer la conception de nos processeurs actuels ? Comment l'utiliser pour concevoir les ordinateurs de demain ? Comment les construire et les utiliser ? Telles sont les questions auxquelles ce mémoire de recherche tentera de répondre.

Table des matières

1 Définition du sujet **6**

1.1 L'informatique quantique 6

1.2 La problématique 7

1.2.1 La recherche sur le calcul quantique 7

1.2.2 La recherche sur les processeurs quantiques 8

1.3 Le contexte de la recherche sur les calculateurs quantiques 8

1.3.1 Une recherche ancienne 8

1.3.2 Un nouvel essor depuis 1994 8

1.3.3 Les acteurs de la recherche 9

1.3.4 Les disciplines concernées 9

1.4 La méthodologie de recherche 9

1.4.1 Les sources documentaires 10

1.4.2 Les interviews 10

2 Introduction aux ordinateurs quantiques **12**

2.1 Impact des phénomènes quantiques sur les processeurs classiques 13

2.1.1 Une question d'échelle 13

2.1.2 Des valeurs discrètes 14

2.2 Le calcul à l'échelle quantique 19

2.2.1 Les qubits 19

2.2.2 Le parallélisme quantique 20

2.2.3 Une information non copiable, mais transportable 21

2.2.4 Une information à la durée de vie limitée 21

2.3 Les requis pour le processeur quantique 22

2.4 La réalisation d'un processeur quantique 23

2.4.1 Les portes quantiques 23

2.4.2 Les critères de DiVincenzo 23

2.5 Bilan de l'introduction 25

3 L'état de la recherche sur les algorithmes quantiques 26
3.1 L'algorithme de Deutsch-Jozsa . . . 27
3.2 L'algorithme de Shor . . . 28
3.2.1 Calcul de la période d'une fonction . . . 28
3.2.2 Utilisation en cryptographie . . . 30
3.3 L'algorithme de recherche de Grover . . . 31
3.3.1 Les limitations de l'algorithme de recherche de Grover . . . 32

4 Les processeurs quantiques 33
4.1 La résonance magnétique nucléaire . . . 33
4.1.1 Présentation de la méthode . . . 33
4.2 Le travail d'Isaac L. Chuang . . . 34
4.3 Les défauts de cette technique . . . 35
4.4 Le qubit optique . . . 35
4.5 La technique des ions piégés . . . 36
4.6 D-Wave . . . 37
4.7 Les circuits supraconducteurs . . . 38
4.7.1 Les propriétés des supraconducteurs . . . 38
4.7.2 Le quantronium . . . 38
4.8 Les principaux problèmes . . . 39
4.8.1 La durée de vie du processeur . . . 39
4.8.2 Le problème de l'échelle . . . 40

5 Description des améliorations 42
5.1 Améliorations souhaitables . . . 42
5.2 Recherche d'axes d'améliorations . . . 43
5.2.1 La similitude avec les superordinateurs . . . 43
5.2.2 Comment exploiter cette similitude . . . 45
5.3 Les axes retenus . . . 45
5.3.1 Les deux axes retenus . . . 45
5.3.2 La justification de ce choix . . . 46
5.4 Description détaillée . . . 46
5.4.1 L'amélioration des processeurs actuels . . . 46
5.4.2 La réalisation d'unités de calcul quantique . . . 47

6 Le processus de changement **49**
6.1 Description du processus 49
6.1.1 Évolution du logiciel 49
6.1.2 Création d'une nouvelle technologie de programmation 49
6.1.3 Adaptation du matériel 50

7 Les apports du travail **52**

8 La conclusion et les perspectives d'avenir **53**

9 Interviews d'experts **57**
9.1 Interview du Docteur Daniel Esteve 57
9.2 Contenu de l'interview 58
9.3 Interview du Docteur Julia Kempe 62
9.4 Contenu de l'interview 63

Chapitre 1

Définition du sujet

1.1 L'informatique quantique

L'informatique dite quantique est une branche de l'informatique qui est différente de celle, classique, que nous connaissons actuellement. Elle est basée sur l'utilisation de la mécanique quantique pour réaliser et faire fonctionner des ordinateurs d'un genre nouveau. Si ceux-ci n'ont pas encore été réalisés, les ordinateurs quantiques promettent de se distinguer de ceux dont nous disposons aujourd'hui.

La mécanique quantique est déjà présente autour de nous, elle est par exemple à la base du fonctionnement des lasers. Il n'est pas ici uniquement question de réaliser un ordinateur dont les opérations seraient régies par celle-ci. Ce qui est recherché ici est la construction d'un processeur, et d'algorithmes associés, capables d'exploiter certains phénomènes présents uniquement en mécanique quantique. Les contraintes pour pouvoir utiliser ces phénomènes sont suffisamment importantes pour qu'aucun processeur quantique vraiment utilisable n'ait encore pu voir le jour.

Néanmoins, si celui-ci venait à être fabriqué, l'ordinateur quantique serait capable, pour toute fonction $y = f(x)$, de calculer simultanément tous les résultats y pour toutes valeurs de x. Cette capacité est connue sous le terme de parallélisme quantique, elle est la principale raison motivant la recherche en informatique quantique. Pouvoir traiter toutes les possibilités possibles à la fois en un seul "cycle" est d'autant plus intéressant que le nombre de combinaison augmente. En calcul classique il est nécessaire d'avoir autant de "cycles" que de valeurs, d'où un avantage de vitesse indéniable pour le processeur quantique dans ce cas de figure.

Cette recherche est actuellement poursuivie en France et dans le monde, principalement dans des centres de recherches et universités tels que le CEA [1], l'université de Yale, le LRI [2]. Certaines entreprises telles qu'IBM et D-Wave sont aussi connues pour travailler sur le sujet, avec une réserve sur cette dernière.

1. Commissariat à l'Énergie Atomique et aux énergies alternatives
2. Laboratoire de Recherche en Informatique

1.2 La problématique

La miniaturisation des composants et les progrès techniques permettent de réaliser des processeurs de plus en plus performants. En 1965, Gordon Moore, co-fondateur d'Intel, a remarqué que la densité des transistors sur les circuits intégrés a doublé tous les 18 mois depuis leur invention. Cette constatation, connue sous le nom de Loi de Moore, se vérifie toujours aujourd'hui.

Or, cette course à la miniaturisation va finir par rencontrer une barrière. En effet, à un moment donné les différents constituants du circuit intégré ne feront plus que quelques atomes d'épaisseur. À partir de ce moment, il ne sera plus possible de décrire le comportement des composants à l'aide de la mécanique classique. Une fois descendu en dessous d'une certaine échelle, seule la mécanique quantique peut être utilisée pour décrire les phénomènes physiques. Les lois qui régissent ces deux types de physique sont suffisamment différentes pour que l'on puisse parler d'un mur séparant deux mondes.

La question qu'il faut naturellement se poser est donc :

Comment construire un ordinateur qui fonctionne de l'autre côté de cette "barrière" ?

Cette problématique est en réalité double, elle suppose, ainsi, d'être tout d'abord capable de construire un tel ordinateur. Celui-ci devrait avoir un processeur dit quantique. Mais elle implique aussi d'être capable de l'exploiter.

Ainsi, de la même façon que la transition, sur les ordinateurs "classiques", d'une architecture de 32 bits vers une architecture à 64 bits a nécessité l'adaptation des logiciels, la programmation d'un ordinateur quantique impliquerait une approche différente de celle utilisée actuellement. Une évolution du *hardware* (matériel) requiert une adaptation du *software* (logiciel).

Cette constatation pousse à attaquer la problématique sous deux angles différents. Chaque angle répondra à une sous-problématique, correspondant respectivement au côté logiciel et au côté matériel. Mais avant de pouvoir entrer dans le vif du sujet, il sera nécessaire d'avoir au préalable une introduction parlant de la mécanique quantique, et ce pour mieux comprendre les phénomènes dont il sera fait part, et leurs impacts sur la manière de calculer.

1.2.1 La recherche sur le calcul quantique

Cette partie traitera de l'aspect logiciel de l'informatique quantique. Il y sera vu les quelques algorithmes déjà mis au point et ce qu'ils apportent par rapport à l'approche traditionnelle. La technologique quantique n'aurait ainsi aucun futur s'il n'était pas possible de l'exploiter au niveau logiciel pour créer des programmes bien plus performants que ceux actuels. Mais le faible nombre d'algorithmes quantiques créés indique qu'il n'est pas aisé d'en réaliser. Ainsi, *qu'apportent les algorithmes quantiques et pourquoi est-il difficile d'en réaliser ?*

Bien que paraissant sortir du périmètre de ce mémoire, qui a été défini comme suit : « *L'informatique quantique est une technologie du futur, quels bénéfices peut-on en attendre pour les microprocesseurs de demain ?* », cette sous-problématique demeure essentielle. En effet, il faut d'abord démontrer que cette technologie est exploitable avant de pouvoir en attendre des bénéfices.

1.2.2 La recherche sur les processeurs quantiques

Cette seconde partie concernera l'aspect matériel. Elle traitera des voies de recherches actuellement exploitées pour tenter de mettre au point un ordinateur quantique. Une fois démontrée la faisabilité au niveau logiciel, il paraît logique de vouloir s'assurer qu'il peut être réalisé un support matériel pour faire tourner ces algorithmes. Si des résultats ont été obtenus, comme en 2001 lorsque l'algorithme de Shor, du nom de son créateur, a pu être testé sur un prototype de processeurs quantiques, la recherche est loin d'être terminée. Il est ainsi utile de se demander *quelles ont été les réussites et les échecs dans les tentatives pour mettre au point un processeur quantique ?*. Ce n'est qu'ainsi que nous pourrons nous faire une idée de a quoi ceux-ci pourraient ressembler une fois qu'ils seront au point.

1.3 Le contexte de la recherche sur les calculateurs quantiques

1.3.1 Une recherche ancienne

La recherche sur les processeurs quantiques a débuté il y a maintenant quatre décennies. La première publication sur un calculateur qui utiliserait les propriétés de la mécanique quantique date en effet du début des années 1970. Elle est due au mathématicien russe Alexander Holevo. Il prouva notamment que l'équivalent du bit au niveau quantique ne peut pas porter plus d'informations qu'un bit classique [Hol73]. Plusieurs autres publications ont suivi durant les années 70.

À l'origine cette recherche étaient purement théorique. La technologie étaient loin de permettre la miniaturisation nécessaire. Cependant la loi de Moore était déjà énoncée. Les scientifiques se sont donc posés la question de la limite de celle-ci. Jusqu'où pourra aller la miniaturisation des composants ? Que se passera-t-il lorsque sera franchie la frontière entre physique classique et physique quantique ?

1.3.2 Un nouvel essor depuis 1994

La recherche sur le calcul quantique a pris un nouveau départ en 1994 avec l'algorithme de Shor. La démonstration que le calcul quantique peut accélérer de façon exponentielle un calcul classique a déclenché un nouvel élan dans le côté mathématique de la recherche quantique, élan qui s'est propagé à l'aspect matériel. Pour la première fois il était prouvé que non seulement il

était possible d'utiliser la mécanique quantique pour un calcul pratique. De plus il était démontré que les contraintes liées à la mécanique quantique pouvaient être contournées.

> « *The recent excitement in this lively and speculative domain of research was triggered by Peter Shor (1994) who showed how a quantum algorithm could exponentially "speed-up" classical computation and factor large numbers into primes much more rapidly (at least in terms of the number of computational steps involved) than any known classical algorithm. Shor's algorithm was soon followed by several other algorithms that aimed to solve combinatorial and algebraic problems, and in the last few years theoretical study of quantum systems serving as computational devices has achieved tremendous progress.[...] Consequently, experimentalists around the world are engaged in tremendous attempts to tackle the technological difficulties that await the realization of such a large scale quantum computer.* » [Hag11]

Une fois prouvé que les systèmes quantiques peuvent être utilisés pour réaliser des calculs mathématiques exploitables ceci à vraiment lancer la recherche sur l'aspect technologique.

1.3.3 Les acteurs de la recherche

Actuellement les acteurs de la recherche pour les processeurs quantiques s'inscrivent en trois catégories principales :

- Les industriels, comme IBM et D-Wave.
- Les organismes de recherche, tels que le groupe Quantronics du CEA, où travaille le Docteur Daniel Esteve.
- Les laboratoires de recherche des universités. Nous pouvons citer l'équipe du Professeur Chuang au M.I.T., les universités de Yale, Santa Barbara, Bristol, Delft. Pour la France peuvent être cités les unités mixtes de recherches du LRI et LIAFA, rattachés à la fois à des universités et au CNRS.

1.3.4 Les disciplines concernées

Même si des industriels y participent, IBM ayant été cité, cette recherche reste actuellement plus dans une démarche scientifique que technique. Les disciplines auxquelles elle fait appel couvrent aussi bien la physique classique, la physique quantique, les statistiques, l'algorithmique que les sciences informatiques.

1.4 La méthodologie de recherche

Pour mener à bien ce sujet de recherche il a été nécessaire de réaliser une étude approfondie. Il a ainsi fallu apprendre les bases de la physique quantique. Il a ensuite été requis de se renseigner sur l'état de l'art de l'informatique quantique.

1.4.1 Les sources documentaires

La première chose faite fut d'acquérir un livre d'introduction à l'informatique quantique [Mer07], en version électronique Kindle. Celui-ci a permis de mieux comprendre ce qu'est réellement l'informatique quantique. Ce livre écrit en anglais se veut une introduction concise, et relativement accessible, sur ce sujet. Il se concentre sur l'aspect algorithmique de l'informatique quantique.

Ensuite il a été recherché dans les anciens articles des Clefs du CEA, et des Défis du CEA, si l'un d'entre eux se révélait pertinent pour le mémoire. La recherche ne fut pas vaine puisqu'un numéro de 2005 des Clefs du CEA contenait un article/dossier sur la question [Est05]. Un article des Défis du CEA, parut pendant la rédaction du mémoire, fut également intéressant [Gan11]. Si l'article porte sur la supraconductivité, une partie fait mention de l'usage de celle-ci pour tenter de créer un processeur quantique.

Puis, bien que succinct, un article paru au début de l'année 2011 dans le magazine international du CNRS [CNR11], parle des ordinateurs quantiques comme étant « *The Ultimate Challenge* ». Cet article démontre bien que l'informatique quantique n'est pas au point et qu'il existe toujours un doute quant à son utilisabilité.

Si Wikipedia ne peut être utilisé comme source documentaire, les contenus n'étant pas assez fiable, les articles dessus peuvent donner des pistes pour la recherche d'informations. Ainsi, la page `http://en.wikipedia.org/wiki/Quantum_computer` comporte des références vers des sites et des articles qui eux sont fiables [Div00] [VYC00]. Cette page contient également une liste de techniques tentées pour créer un processeur quantique. Elle a permis de connaître des noms de voies de recherches actuellement poursuivies pour pouvoir voir en quoi elles consistent et se renseigner plus amplement sur elles par la suite.

1.4.2 Les interviews

Afin de mener à bien ce mémoire, il était important d'interviewer au moins deux chercheurs travaillant dans des laboratoires de recherche français. Lors de la phase de recherche documentaires, certains noms sont apparus plusieurs fois. Il était aussi préférable que les interviews permettent de couvrir les deux sous-problématique.

Tout d'abord, le Docteur Daniel Esteve à été rencontré, c'est l'un des fondateurs du groupe Quantronics. Par ses réponses, il a permis d'acquérir une meilleure compréhension de l'aspect physique de la problématique. Il a également eu la courtoisie de me faire visiter les laboratoires du groupe Quantronics.

Finalement, un entretien téléphonique avec le Docteur Julia Kempe. Cette ancienne membre du Laboratoire de Recherche en Informatique d'Orsay travaille actuellement au LIAFA [3]. Elle a pu aider à mieux comprendre l'aspect algorithmique de la problématique. Cette seconde interview fut complémentaire de la première. En effet, ainsi les deux sous-problématiques ont

3. Laboratoire d'Informatique Algorithmique : Fondements et Applications

bien été couvertes et certains aspects ont pu être discuttés avec les deux interviewés, tels que l'utilisabilité de l'informatique quantique.

Chacune de ces interviews à donner lieu à un compte rendu, situé en annexe du mémoire, pages 57 et 62 respectivement pour les Docteurs Esteve et Kempe.

Chapitre 2

Introduction aux ordinateurs quantiques

L'informatique quantique est encore en gestation. Comme il le serra vu au cours de ce mémoire, une longue route reste encore à parcourir avant de réaliser un ordinateur quantique utilisable.

Ainsi, si des prototypes de processeurs quantiques ont été mis au point dès les années 90 [1], ceux-ci ne sont pas encore suffisamment viables. Ils ont en effet une durée de vie très courte, et ils restent trop petits [2] pour être réellement exploitables. Un autre problème des prototypes réalisés jusqu'à ce jour concerne la lecture des résultats. Il est plus difficile d'arriver à retrouver le résultat d'un algorithme quantique que d'arriver à faire tourner cet algorithme. Pour cette raison, il est parfois préférable de parler de calcul quantique et non d'informatique quantique. Effectivement, contrairement au terme d'informatique, celui de calcul n'implique pas que l'on sache lire le résultat.

Ensuite, afin de pouvoir appréhender pourquoi l'ordinateur quantique est le rêve des chercheurs en informatique, deux points sont à considérer :

– En premier lieu, comme son nom le suggère, l'ordinateur quantique se base sur la branche de la physique appelée mécanique quantique. Une compréhension minimale des phénomènes qui entrent en jeu est nécessaire. Il est surtout important de saisir les différences entre mécanique classique et mécanique quantique.

– Ce n'est qu'ensuite qu'il est possible de comprendre les différences fondamentales entre l'informatique "classique" et celle dite quantique. De cette façon il sera mis également en valeur en quoi cette dernière est intéressante.

Cependant la mécanique quantique n'est pas le sujet de ce mémoire, c'est pourquoi il n'en sera donné ici qu'un aperçu, utile et suffisant à la compréhension. Dans cette partie, il sera fait autant que possible l'usage d'analogies, celles-ci n'auront pas la prétention d'être le plus juste possible, mais seulement de donner une vision d'ensemble suffisante pour la compréhension du reste du mémoire.

1. Ces prototypes seront décrits dans la suite du mémoire.

2. Lorsque l'on parle de la taille d'un processeur quantique, on ne décrit pas ses dimensions physiques mais la largeur des données sur lesquelles il peut travailler, de la même façon qu'il existe des processeurs classiques en 32bits et d'autres en 64bits.

2.1 Impact des phénomènes quantiques sur les processeurs classiques

2.1.1 Une question d'échelle

La mécanique quantique correspond aux lois qui régissent la matière à l'échelle des particules. Il s'agit d'une branche de la physique utilisée pour décrire et étudier ce qui se passe au niveau des atomes et des particules élémentaires. Par opposition, à notre échelle nous utilisons la mécanique dite Newtonienne, ou classique.

Analogie avec le comportement humain

Pour être rigoureux, dire que mécaniques quantique et classique obéissent à des règles différentes n'est pas tout à fait exacte. Tout élément physique obéit au final aux lois de la mécanique quantique. Les lois à notre échelle peuvent être considérées comme une version simplifiée de celles au niveau des particules.

L'analogie suivante va servir à démontrer pourquoi, dans certains cas, un changement d'échelle peut impliquer un changement des "lois" utilisées pour décrire un systèmes.

Ainsi, si nous prenons un être humain comme exemple. L'observation de son comportement montrera des différences entre les moments où il se pensera seul, et les moments où il sera en société. Il s'agira pourtant du même individu, sa personnalité n'aura pas changé. Dans le cas de la mécanique, tout comme pour le cas du comportement, il s'agit d'une question d'échelle. De la même façon que les sciences comportementales distinguent :

- la sociologie, étude du comportement d'une société
- la psychologie, étude du comportement d'un individu donné

La mécanique est séparée entre :

- celle dite classique, étude des phénomènes regardés dans un ensemble
- celle dite quantique, étude des phénomènes à l'échelle des particules

Il existe en réalité d'autres types de physique, comme la relativiste, mais celles-ci n'entrent pas en ligne de compte pour ce sujet.

Impact sur la fabrication des processeurs

Ce changement de règles entre l'échelle classique et celle quantique, aura obligatoirement des conséquences sur les processeurs. Actuellement un processeur fonctionne correctement tant que les différents transistors qui le composent se comportent de la façon dont ils le devraient. Or si la miniaturisation des composants se poursuit, il arrivera le moment ou cela changera. Lorsque les transistors et les pistes du circuit ne feront plus que quelques atomes d'épaisseurs, le comportement individuel des atomes sera à prendre en compte. Or ceux-ci, comme les êtres humains, ne peuvent plus être considérés de la même manière lorsqu'ils sont pris isolés.

La conséquence est que le comportement des processeurs, tels que nous les concevons aujourd'hui, ne sera plus le même à cette échelle. Il s'agit ici donc bien d'un véritable mur qui se dresse à l'horizon, sur le chemin de la miniaturisation.

2.1.2 Des valeurs discrètes

Dans les processeurs classiques : les bits

Dans l'informatique telle que nous la connaissons, l'information est modélisée à l'aide d'une unité élémentaire appelée le bit. Celle-ci peut prendre deux valeurs, 0 ou 1. C'est à dire qu'un bit est soit dans l'état 0 soit dans l'état 1, et qu'il n'existe pas d'état possible intermédiaire. Le bit est une donnée dite discrète, car son état appartient forcément à un ensemble fini de valeurs. Par opposition on parle de donnée continue lorsque l'état appartient à un intervalle, cf. illustration 2.1.

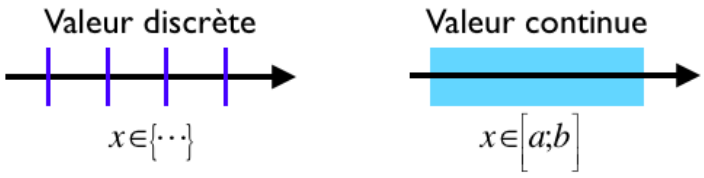

ILLUSTRATION 2.1 – À gauche une valeur discrète, à droite une valeur continue

Cette donnée discrète, qu'est le bit, est en réalité obtenue par discrétisation d'une donnée continue : la tension électrique. Il est établi que si la différence de potentielle est dans une plage autour d'une première valeur de référence, gnd pour la terre, alors le bit est considéré comme étant à 0. De même, la tension de référence vcc sert à établir l'état 1. Comme la tension n'a pas besoin d'être strictement égale à une des tensions de référence, mais peu osciller légèrement autour, ceci offre une certaine tolérance au bruit.

Ainsi, si les perturbations extérieures, telles que les radiations et les champs magnétiques, induisent une modification qui reste suffisamment proche d'une valeur de référence, l'information n'est pas perdue. Une valeur "1" qui serait modifié en quelque chose entre 0.9 et 1.1 serait traitée comme un "1". Cette "stabilité" de l'information est essentielle pour garantir la valeur des résultats lors de calculs.

Le problème du bruit

Il existe cependant des cas où les perturbations sont suffisamment importantes pour que l'information soit altérée, une valeur 0 peut ainsi être transformée en une valeur 1. Ce phénomène est connu sous le terme de SEU, Single Event Upset. Il est très rare, voir négligeable au niveau du sol. Il concerne surtout les avions et les satellites, en raison du rayonnement solaire et de l'ionisation de l'atmosphère en haute altitude.

À l'heure actuelle les SEUs restent suffisamment rares pour que les fabricants des microprocesseurs, que nous trouvons dans nos ordinateurs ou téléphones, puissent se permettent de les ignorer. La valeur d'une information étant stable, si un même calcul est répété n fois sur m machines différentes, il est obtenu $n * m$ fois le même résultat. Cette fiabilité des calculs est primordiale pour l'informatique telle que nous la connaissons.

Il est néanmoins connu que les SEUs deviennent de plus en plus probables à mesure que l'on progresse dans la miniaturisation. En effet, à mesure que la taille des pistes se réduit, le nombre d'électrons, qui véhiculent l'information, diminue. Une perturbation extérieure peut alors plus facilement provoqué un SEUs. L'augmentation de la densité des circuits risque ainsi de rencontrer un premier obstacle avant même d'arriver à l'échelle quantique.

Les valeurs discrètes dans le domaine quantique

Si à l'échelle classique les processeurs utilisent un "support continue" pour y placer une donnée discrète, il n'est pas possible de faire de même au niveau quantique. En effet, à cette échelle le niveau d'énergie n'est plus une donnée continue, mais une donnée directement discrète. Ceci a été mis en évidence dès le début du XXème siècle. Il existait alors un problème théorique que la mécanique classique était incapable de résoudre, celui dit du corps noir.

> Le terme de corps noir désigne un objet capable d'absorber tout rayonnement qui lui parviendrait, quel que soit la nature du rayonnement. Un tel objet ne réfléchirait pas la lumière, ce qui lui a donné son nom de corps noir. En réalité ce corps ne serait pas totalement noir. En effet s'il absorbe des rayonnements, cela implique qu'il chauffe. Or tout corps chauffé émet des rayonnements, c'est le principe même des lampes à incandescence.
>
> Plus la température du corps augmente et plus la largeur du spectre sur lequel il émet des rayonnements augmente. Ceci explique qu'une étoile bleue soit plus chaude qu'une étoile rouge.

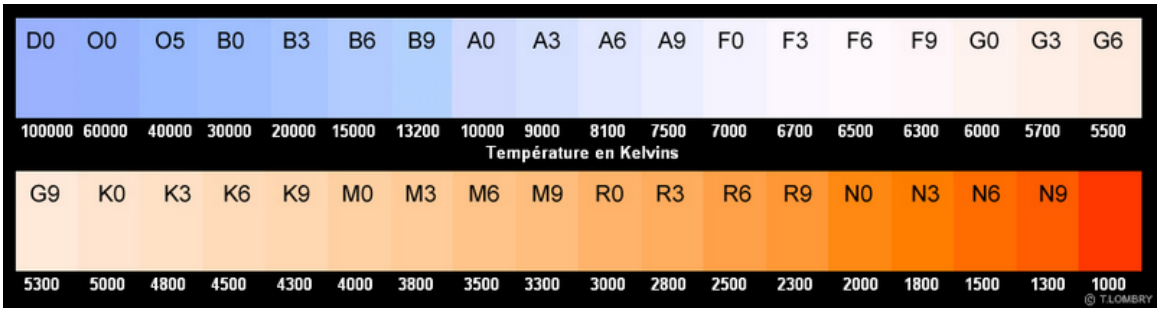

ILLUSTRATION 2.2 – Couleur et classification des étoiles en fonction de leur température de surface

> De plus, les raies d'émissions d'un corps chauffé correspondent aux raies d'absorptions de ce même corps. Un corps noir émettrait donc sur un spectre continu.

Le problème qui se posait alors est que les calculs démontraient qu'un corps noir serait capable d'émettre une quantité infinie d'énergie, ce qui est par essence impossible.

Le physicien Max Planck proposa une solution à ce problème. Il postula que les atomes ne sont pas capables d'échanger une quantité quelconque d'énergie, mais seulement des quantités de valeur discrète. Par cela, on entend qu'il existe des paliers et que les échanges ne peuvent être réalisés que pour des valeurs correspondantes à un palier.

Plank parlait de quantités d'énergies pour décrire ce phénomène. Son hypothèse fut alors appelée théorie des quantas. Elle est maintenant intégrée à part entière dans la mécanique quantique dont elle est un des fondements.

Les conséquences d'avoir des valeurs discrètes, et non continues, offrent des applications dans la vie de tous les jours. Elles permettent notamment le fonctionnement des lasers [3]. Elles sont également essentielles pour l'informatique quantique, car elles impliquent que certaines propriétés quantiques mesurées ne peuvent prendre que certaines valeurs bien définies. Ceci permet d'utiliser ces propriétés comme support d'information dans un processeur quantique, comme nous le verrons par la suite.

Mais il existe aussi une autre implication, dommageable, pour les processeurs classiques. Lorsqu'on approche du domaine quantique, la zone de tolérance, autour des valeurs de références pour le 0 et le 1 disparaît. En effet, ces zones ne pouvaient exister que tant que nous étions dans un domaine continu. Avec leur disparition, la probabilité d'avoir un phénomène SEUs augmente, car une perturbation pourrait faire directement basculer une valeur "1" à une valeur "0", voir à une valeur "2", inutilisable. La valeur des résultats devient alors incertaine.

L'incertitude en mécanique quantique

Le manque de garanties sur la valeur des résultats n'est pas uniquement lié à la disparition des zones de tolérance. Elle est aussi ancrée au coeur même de la mécanique quantique.

Le principe d'incertitude d'Heiseinberg

Il tient son nom du physicien allemand Werner Karl Heisenberg, lui aussi un des fondateurs de la mécanique quantique.

Ce principe, énoncé en 1927, veut que les valeurs associées à certains couples de propriétés ne puissent être connues de façons précises pour les deux éléments du couple à la fois. Il n'est ainsi pas possible de connaître précisément à la fois la vitesse et la position d'une particule. Ceci explique pourquoi dans le modèle quantique les électrons sont représentés comme un nuage autour de l'atome, voir illustration 2.3.

3. Dans un laser, les atomes présent dans la "cavité" sont excités par absorption d'un photon permettant de les faire monter d'un niveau d'énergie. Lorsqu'un second photons arrive, avec la même énergie, alors l'atome revient dans son état initial en émettant deux photons

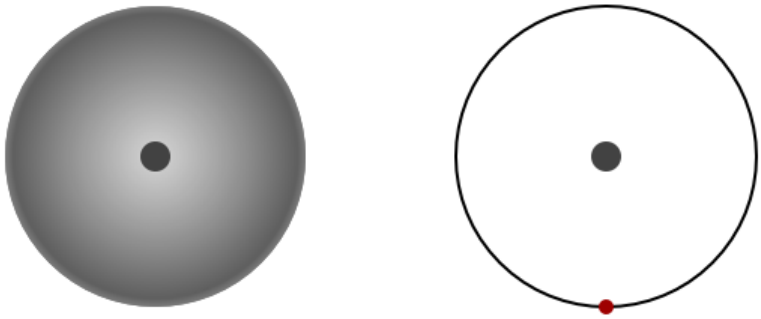

ILLUSTRATION 2.3 – Représentation d'un électron autour d'un atome : à gauche le modèle quantique, à droite le modèle classique.

Cette incertitude se retrouve aussi, comme nous allons le voir, dans la valeur des propriétés quantiques discrètes.

La superposition quantique

La superposition quantique, aussi nommée état superposé, est représentée par la notation de Dirac $|\psi\rangle$. Elle n'est pas un état à proprement parler. Il s'agit d'une incertitude quand à l'état dans lequel se trouve une propriété discrète. Celle-ci a des conséquences directes sur la façon dont l'information peut être représentée dans le domaine quantique.

Dans le cas d'une propriété pouvant prendre deux valeurs, ici $|0\rangle$ et $|1\rangle$, elle est représentée par la formule $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Bien que le mémoire porte sur l'informatique quantique et que par là même nous ne considérerons que des propriétés ne pouvant prendre que deux états, il faut noter que la superposition d'états s'écrit en réalité comme la somme coefficientée des différents états que peut prendre la propriété. Nous avons alors comme formule $|\psi\rangle = \sum_i \alpha_i\,|i\rangle$ avec i le nombre d'états possibles et $|i\rangle$ l'état i. Ce phénomène de superposition quantique implique que la logique booléenne, basée sur deux états incompatibles, ne peut plus être employée.

Pour mieux comprendre ce phénomène, nous allons parler d'une expérience assez célèbre en physique quantique.

Le chat de Schrödinger

L'expérience dite du chat de Schrödinger (illustration 2.4) n'a en réalité jamais été réalisée [Bud] [Jon]. Il s'agit uniquement d'une expérience théorique imaginée en 1935 à titre de démonstration. Elle tient son nom du physicien autrichien Erwin Schrödinger, lui aussi considéré comme étant un des pères de la mécanique quantique.

Cette expérience permet à la fois une description de l'état de superposition et de démontrer que celle-ci ne peut exister à l'échelle macroscopique. L'objectif de E. Schrödinger avec cette

vue de l'esprit était de montrer son désaccord avec la vision de l'époque selon laquelle la mesure ne détruit pas la superposition quantique.

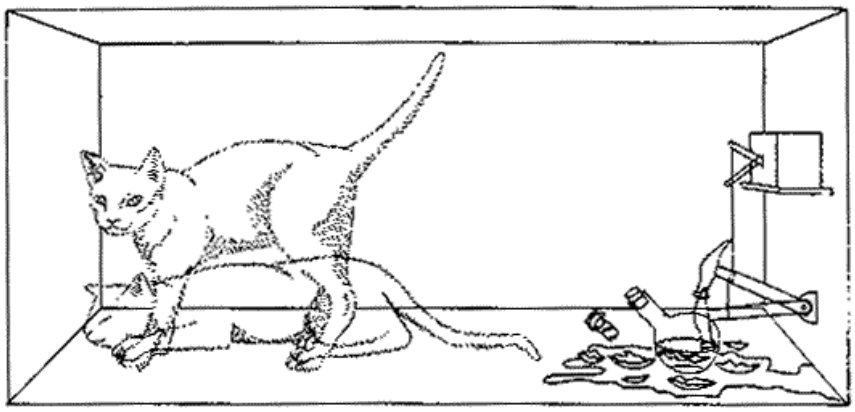

ILLUSTRATION 2.4 – Le chat de Schrödinger : mort et vivant à la fois

Soit un chat, considérons que son état vaut $|0\rangle$ s'il est mort et $|1\rangle$ s'il est toujours en vie.

Ce chat est placé dans une boîte fermée, sans possibilité d'en voir le contenu depuis l'extérieur. Dans cette boîte est aussi placé un dispositif destiné à dégager du poison en cas de détection de la désintégration d'un atome.

Le dispositif est prévu pour ne fonctionner que pendant un temps limité pendant au terme duquel il existe 50 % de probabilité qu'il se soit déclenché.

Une fois l'expérience lancée, il est impossible de savoir l'état du chat. La probabilité qu'il soit encore en vie est alors égale à la probabilité que le poison n'ait pas été libéré, et la probabilité qu'il soit mort est égale à celle que le poison ait été libéré.

Or la libération du poison est un élément aléatoire. Si l'on peut calculer les probabilités, il n'est pas possible d'être certain.

À tout instant on peut alors dire du chat qu'il est mort avec a % de probabilité et vivant avec b % de probabilité, $a + b = 100$ %. Une fois le dispositif désactivé, a et b vaudront 50 %. On dit qu'il est dans un état superposé, à la fois en vie et mort.

Seule l'observation directe du chat, la "mesure", permet de connaître son véritable état, mais cela fait passer d'une superposition quantique à un état discret. En effet, toute nouvelle mesure redonnera le même résultat, soit le chat était vivant et il l'est toujours, soit il était mort à la première mesure et il l'est toujours aussi.

Cette expérience démontre bien deux choses, à savoir :
– que l'état superposé ne peut exister à l'échelle macroscopique, en effet il est impossible d'avoir un chat qui soit à la fois mort et vivant,

– que la mesure a bien modifié l'état du système, il était dans une superposition quantique et il est maintenant dans un état définit.

L'existence de cette superposition d'états démontre bien que le calcul classique, basé sur des bits, ne peut être utilisé passé un certain stade de miniaturisation. En l'absence de valeurs 0 et 1 stables, il est impossible de garantir les résultats, ce qui va à l'encontre des fondements de l'informatique. Il existe néanmoins la possibilité d'exploiter le fait d'avoir à la fois 0 et 1 pour réaliser des calculs sur les deux valeurs à la fois. C'est ici que l'informatique quantique intervient.

2.2 Le calcul à l'échelle quantique

2.2.1 Les qubits

Si l'unité d'information élémentaire pour l'informatique classique est le bit, dans le domaine quantique, on parle de bit quantique, ou qubit voir qbit. Un qubit peut être dans un état $|0\rangle$, un état $|1\rangle$ ou dans une superposition d'états, $|\psi\rangle$. Dans ce dernier cas on considère que sa valeur est simultanément $|0\rangle$ et $|1\rangle$. Plutôt que de craindre cette particularité, il est possible de l'exploiter, même si cela requiert de changer l'approche de l'informatique.

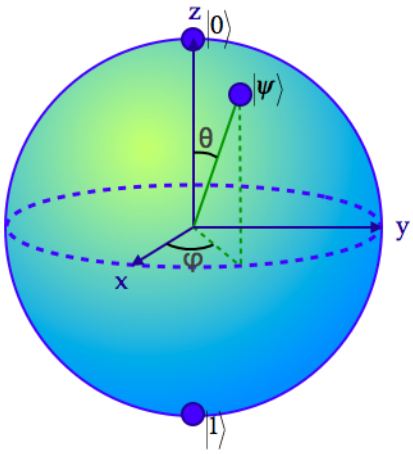

ILLUSTRATION 2.5 – La sphère de Bloch

Les qubits sont généralement représentés à l'aide de la sphère de Bloch (Illustration 2.5). Celle-ci permet de représenter un système quantique à deux niveaux, c'est-à-dire une propriété de la mécanique quantique dont la mesure ne peut donner que deux valeurs possibles. Ces deux valeurs sont sur l'axe des ordonnés, respectivement en haut et en bas de la sphère.

La superposition d'état, combinaison des états $|0\rangle$ et $|1\rangle$, correspond à la formule $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. α et β sont des nombres imaginaires tels que $\alpha^2 + \beta^2 = 1$. Pour simplifier il peut être considéré que α est la probabilité d'être dans l'état $|0\rangle$ lors de la lecture et β est celle d'être dans l'état $|1\rangle$. Il faut en effet savoir que si le qubit peut être dans un état de superposition, la lecture de sa valeur donnera toujours un résultat discret, c'est-à-dire soit un $|1\rangle$, soit un $|0\rangle$. Tant qu'il n'a pas été lu le qubit est considéré comme étant à la fois à 0 et à 1, tout comme le chat

était à la fois mort et vivant. Mais là où l'expérience de Schrödinger était prévue pour avoir des probabilités équiprobables, les probabilités de lire le qubit comme étant dans l'état $|1\rangle$ ou dans l'état $|0\rangle$ ne sont pas nécessairement égales. Une fois la lecture réalisée sur un qubit, toute nouvelle lecture redonnera le même résultat tant que le qubit n'aura pas été réutilisé pour un autre calcul. Le chat reste mort ou il reste vivant mais sont état ne change pas une fois que l'observation à été faite.

2.2.2 Le parallélisme quantique

Cette possibilité d'être dans deux états en même temps offre une capacité unique, connue sous le nom de parallélisme quantique. Réaliser une opération sur un qubit est équivalent à réaliser une même opération, dans le monde classique, sur un bit à 0 et sur un second à 1. Si le nombre est sur deux qubits, cela revient alors à réaliser quatre opérations à la fois, huit pour 3 qubits, etc. À chaque fois que la taille d'un nombre est augmentée de 1 qubit, le nombre d'opérations équivalent est doublé.

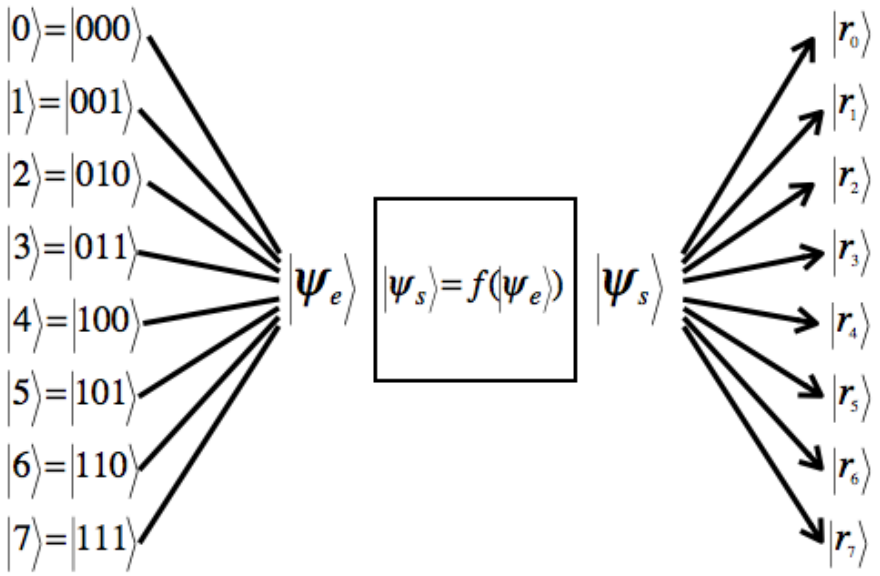

ILLUSTRATION 2.6 – Parallélisme quantique : calcul réalisé sur 3 qubits.

Alors que pour un processeur classique l'augmentation de la taille d'un nombre signifierait l'augmentation du nombre d'opérations pour un calcul portant sur toutes les combinaisons, il n'en est rien dans le domaine quantique. L'accélération est théoriquement exponentielle. Théoriquement seulement car dans les faits, un seul des résultats n'est lisible à la fois. Il faut recommencer l'expérience plusieurs fois pour lire les autres résultats, sans possibilité de choisir quel résultat sera lu.

2.2.3 Une information non copiable, mais transportable

Alors que l'information peut être recopiée dans un processeur classique, ceci n'est pas possible avec les qubits. Il faudrait être capable de connaître précisément les valeurs de α et de β pour pouvoir reproduire l'information, or ces valeurs ne peuvent être obtenues directement. Pour pouvoir les estimer, il faudrait recommencer la même série d'étapes un grand nombre de fois. En réalisant des statistiques sur les valeurs lues, il serait alors possible d'estimer les valeurs de α et β, mais sans jamais connaître leur valeur exacte.

Cette impossibilité de copier la valeur d'un qubit implique qu'il est impossible de garder de résultats intermédiaires, ce qui limite d'autant plus l'utilisation du parallélisme quantique décrit précédemment.

Il est néanmoins possible de déplacer l'information, c'est-à-dire de la faire passer d'un qubit à un autre, et ce grâce à l'intrication quantique. Il s'agit d'un phénomène qui veut que si deux particules ont interagi l'une avec l'autre, alors il se forme un lien entre elles. Par la suite, et quelque soit la distance qui les sépare, la mesure d'une ou de plusieurs propriétés quantiques de l'une des particules permet de connaître instantanément l'état, pour ces mêmes propriétés, de la seconde particule.

Il devient ainsi possible de transporter un état quantique d'une particule à une autre, c'est ce que l'on appelle la téléportation quantique [QOG]. Ce phénomène n'est cependant pas la réalisation d'une copie d'un état quantique. Le processus utilisé détruit en effet l'état quantique initial du premier qubit. De plus, cette opération requiert également l'utilisation de moyens de communications "classiques" pour fonctionner, la transmission de l'état ne peut donc pas être tout à fait considérée comme instantanée.

Actuellement utilisé dans le cadre de la cryptographie quantique, ce phénomène est aussi utilisé comme base pour les travaux sur les processeurs quantiques [Asp]. Cette opération de téléportation quantique est l'équivalent de l'opération de décalage, shift, présente dans nos microprocesseurs. Celle-ci étant indispensable pour la réalisation de multiplications et de divisions, on comprend pourquoi son équivalent quantique a une grande importance. Elle est aussi utilisée pour que 2 qubits disctincts puissent être utilisés pour former un ensemble à 2 qubits.

2.2.4 Une information à la durée de vie limitée

Le terme de décohérence fut proposé en 1970 par le physicien allemand Heinz-Dieter Zeh. Il désigne un phénomène au cours duquel un élément qui obéissait aux règles de la mécanique quantique diverge vers celle de la physique classique. La décohérence faisant disparaître la superposition d'états, elle fait aussi disparaître l'information du qubit. Par conséquent, il n'est pas possible de conserver une donnée dans le domaine quantique, contrairement à l'informatique actuelle où elle peut être enregistrée dans des mémoires, des disques durs voir des supports optiques.

La décohérence est due au fait que les particules ne sont jamais totalement isolées, elles sont perturbées par leur environnement. De ce fait, la superposition quantique, par essence instable, ne peut être conservée indéfiniment. On utilise le terme de temps de cohérence pour décrire le laps de temps pendant lequel on peut considérer qu'une propriété reste dans le même état de superposition [CNR11].

2.3 Les requis pour le processeur quantique

S'il existe plusieurs voies de recherches pour la réalisation de processeurs quantiques, pour obtenir les qubits utilisés par ses processeurs quatre éléments doivent toujours être présents :
- un "support" pour le qubit,
- une propriété physique mesurable pour ce support,
- un appareil pour influer sur cette propriété,
- un appareil pour lire l'état de la propriété.

Le support pour le qubit

Le support du qubit peut être une particule, un atome, un ion, voir même une molécule [4]. Le support doit être suffisamment petit pour appartenir au domaine quantique, et suffisamment grand pour être isolable et utilisable avec notre technologie actuelle.

Une propriété physique mesurable

Tout comme un bit est créé à l'aide de tensions électriques, le qubit a besoin d'une propriété pour exprimer sa valeur. Le choix de la propriété dépend à la fois des capacités techniques et du support utilisé.

S'il est possible d'utiliser une propriété quantique ne pouvant prendre que deux valeurs, il est également possible d'utiliser une propriété avec plus que deux valeurs. Mais ceci n'est réalisable que si deux des valeurs sont suffisament isolées des autres pour qu'une forte probabilité d'être dans l'une ou l'autre de ces deux valeurs entraîne une probabilité tellement faible d'être dans les autres valeurs que celles-ci puissent être ignorées.

Un appareil pour influer sur cette propriété

Cette contrainte concerne non seulement l'initialisation du système, c'est-à-dire le choix des valeurs de départ du calcul, mais aussi le déroulement du calcul proprement dit.

4. La technologie de la Résonance Magnétique Nucléaire, que nous verrons par la suite, a été utilisée avec des molécules de chloroforme.

Un appareil pour lire l'état de la propriété

Tout logiquement, la réalisation d'un calcul n'a de l'intérêt que si l'on n'est capable de lire le résultat. Cet appareil de lecture ne sera pas capable de retrouver les valeurs de α et β, mais il doit permettre de dire si la mesure à placer le qubit dans un état $|0\rangle$ ou $|1\rangle$.

2.4 La réalisation d'un processeur quantique

2.4.1 Les portes quantiques

Tout comme les processeurs traditionnels sont constitués de portes logiques, leurs pendants quantiques disposent eux aussi d'éléments appelés portes. Celles-ci n'ont pas exactement le même rôle, les opérations NOT, AND, OR,... existants en informatique traditionnelle ne sont pas applicables dans le domaine quantique. Elles permettent de réaliser d'autres types de transformations, représentables grâce au calcul matriciel.

Une porte quantique à un qubit correspond à une rotation de la sphère de Bloch, illustration 2.5 vue page 19, sur elle-même. Les portes élémentaires sont classées en deux catégories : PHASE et ROTATION, selon qu'elles correspondent respectivement à une rotation autour de l'axe z ou de l'axe y [Lac07]. Comme toutes les portes quantiques 1 qubit, simples ou complexes, résultent au final d'une succession de rotations, elles sont par essence réversibles.

Les portes quantiques à deux qubits peuvent elles aussi être classées en deux catégories, selon qu'elles permettent ou non l'intrication des qubits. Dans le cas où il y a intrication, les deux qubits ne peuvent être décrits séparément, car la valeur de chacun d'entre eux dépend de celle de l'autre. Parmi les portes à deux qubits utilisant l'intrication, nous pouvons noter la porte contrôle unitaire, qui est le cas général pour toute porte à deux qubits réalisant une opération élémentaire sur un qubit *cible* lors que le second qubit, *de contrôle*, est dans l'état $|1\rangle$.

Un assemblage composé de portes à un qubit et d'une porte à deux qubits, réalisant l'intrication, est appelé « *un ensemble universel de portes quantiques* » [Lac07].

2.4.2 Les critères de DiVincenzo

Les critères vus précédemment pour la réalisation d'un qubit sont nécessaires mais non suffisant pour la réalisation d'un ordinateur quantique. Ils ne correspondent ainsi qu'au premier des critères dit de DiVincenzo [Div00]. Ceux-ci sont au nombre de 5 et correspondent aux contraintes qui doivent être respectées pour pouvoir créer un processeur quantique :

1. disposer de qubits bien définis,
2. disposer d'une fonction de reset pour faire tomber tous les registres à l'état $|0\rangle$,
3. disposer d'un ensemble universel de portes quantiques,
4. disposer d'une lecture fidèle en un coup,

5. disposer d'un temps de cohérence assez long.

Ces critères s'expliquent relativement facilement.

Disposer d'une fonction de reset

Pour expliquer ce besoin il faut comprendre comment est obtenue la superposition d'états $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec α et β choisis. Pour arriver à définir les valeurs de ces deux coefficients, il n'existe qu'une seule solution possible : il faut partir d'un état où les coefficients sont connus puis il faut modifier l'état associé à la propriété portant le qubit. Par ailleurs, il n'existe que deux états où les coefficients sont connus : $|0\rangle$ et $|1\rangle$. Par essence l'état $|0\rangle$ possède moins d'énergie que l'état $|1\rangle$, or il est plus facile de rajouter de l'énergie que d'en soustraire.

Pour initialiser un qubit dans un état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ voulut, il est donc nécessaire de partir de l'état $|0\rangle$ et de rajouter la quantité d'énergie telle que l'on obtient les coefficients α et β désirés.

Une autre raison d'avoir une fonction de reset, est qu'elle permet d'avoir une source continue d'états $|0\rangle$. Or, ceux-ci sont indispensables pour les circuits de correction d'erreurs quantiques [Div00] [Pou08].

Disposer d'un ensemble universel de portes quantiques

Ce critère reprend le problème de l'échelle vu précédemment. Pour être utilisable un ordinateur quantique devrait posséder un nombre suffisant de qubits, et par là même de portes quantiques pour travailler dessus.

La précision selon laquelle ces portes doivent être universelles est liée aux qubits eux-mêmes. Dans un processeur classique les bits, correspondant aux données travaillées, sont aiguillés au sein du processeur pour passer par les portes logiques nécessaires au calcul demandé. Mais ceci n'est pas possible avec les qubits, en effet cet aiguillage est incompatible avec l'isolement requis pour que le qubit reste dans une superposition d'état. Il est donc nécessaire que chaque porte quantique puisse réaliser toutes les transformations voulues sur les qubits.

Disposer d'une lecture fidèle en un coup

Ce quatrième critère correspond à un problème essentiel. Nous savons que lorsque l'état d'un qubit est lu nous obtenons soit $|0\rangle$ soit $|1\rangle$. La probabilité d'obtenir l'un ou l'autre est théoriquement fonction uniquement des coefficients α et β, mais un processus de lecture non fidèle peut amener à une lecture qui ne respecte pas les probabilités qui auraient dû être obtenues. Une lecture en un coup permet d'obtenir une meilleure fidélité et de réaliser un nombre plus grand d'opérations.

Disposer d'un temps de cohérence assez long

Comme nous l'avons vu précédemment, le temps de cohérence est un facteur important pour un processeur quantique. Il s'agit du temps pendant lequel on peut considérer qu'un système mis dans une superposition d'états $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ possède toujours les mêmes coefficients α et β.

Ce temps de cohérence correspond donc aussi au temps durant lequel nous pouvons être sûrs des conditions de départ d'un calcul quantique. Pour utiliser une analogie, supposons une fonction $y = f(x(t))$ dont nous recalculons la valeur à chaque changement de la variable d'entrée $x(t)$. Si nous voulons pouvoir utiliser les résultats de la fonction, le calcul doit être réalisé plus rapidement que le changement de valeur de $x(t)$.

Le même problème est présent en informatique quantique. Plus le temps de cohérence est grand, c'est-à-dire plus lentement évolue la valeur de $x(t)$ et plus la fonction à calculer peut être complexe.

2.5 Bilan de l'introduction

Il apparaît que s'il reste possible de réaliser des calculs au niveau quantique, ceux-ci ne ressembleraient pas à ceux utilisés dans l'informatique classique. L'exploitation des propriétés offertes par ce nouveau monde devra passer par l'utilisation d'une nouvelle façon de penser et concevoir les programmes. Celle-ci est connue sous le terme d'algorithmique quantique.

Chapitre 3

L'état de la recherche sur les algorithmes quantiques

L'utilisation du parallélisme quantique, rendu possible par la superposition d'états, permet de réaliser des algorithmes dont l'efficacité n'a pas d'équivalent en informatique classique.

Il existe ainsi deux algorithmes qui, avec leurs différentes variations, sont présentés par N.D. Mernin, ancien Professeur de physiques atomiques à l'université américaine Cornell, comme la base du logiciel quantique. Il les a ainsi qualifiés de « the two masterpieces of quantum computational software » dans son livre d'introduction à la science des ordinateurs quantiques [6].

Il s'agit des algorithmes de Shor et de Grover, inventés respectivement en 1994 et 1996.

Comme cela l'a été évoqué précédemment, la difficulté d'exploiter un ordinateur quantique vient de sa nature même. Si un système quantique réalise simultanément les opérations sur toutes les combinaisons possibles, seul le résultat d'une seule de ces combinaisons est lisible à la fois, sans possibilité de choisir laquelle. De plus, chaque lecture d'un résultat détruit le calcul, obligeant alors à recommencer toutes les opérations si l'on veut connaître le résultat pour une autre combinaison.

En plus de ce problème de lecture, survient un autre problème, celui-là est lié aux portes quantiques. Celles-ci ne peuvent en effet réaliser que des opérations réversibles. Ceci implique que même si la superposition d'états n'était pas utilisée et que les qubits étaient toujours maintenu dans des conditions purement $|1\rangle$ ou $|0\rangle$, il faudrait quand même réécrire tous les algorithmes existants. Si l'adaptation des programmes reste possible, elle donne un algorithme de même efficacité que celui de départ, ne donnant alors aucun gain de vitesse. Ceci démontre bien que, pour pouvoir profiter du calcul quantique, il faut changer notre façon de concevoir les algorithmes.

Ce n'est qu'en 1994 que le mathématicien Peter Shor arriva à réaliser le premier véritable algorithme quantique optimisé. Il démontra aussi que, dans certains cas, les algorithmes quantiques peuvent réellement être plus efficaces que ce qu'il est possible de réaliser avec l'informatique classique.

3.1 L'algorithme de Deutsch-Jozsa

Cet algorithme porte le nom de David Deutsch et Richard Jozsa, respectivement un physicien britannique et un mathématicien britanniques. Il est basé sur des travaux de 1985, de D. Deutsch, complétés en 1992 par R. Jozsa. Il fut encore amélioré par la suite en 1998.

L'intérêt de cet algorithme quantique est qu'il fut le premier inventé qui était plus efficace que son pendant classique. Ces travaux ont par la suite inspiré ceux de Shor et Grover.

Description du problème à résoudre

L'algorithme de Deutsch-Jozsa a été réalisé pour caractériser une suite de valeurs binaires. On suppose que les valeurs sont soit toutes les mêmes, soit équilibrées, c'est-à-dire avec une moitié de 0 et une moitié de 1. Il s'agit alors de savoir auquel des deux cas la suite présentée appartient.

En algorithmique classique, il est démontré que le cas où les valeurs sont toutes identiques est le plus long à prouver. Pour N valeurs dans la série, il est nécessaire d'en lire $N/2 + 1$ pour être sûr d'être dans ce cas.

En effet, si la suite est équilibrée, il existe alors deux possibilités notables, une favorable et une défavorable. Pour la première, la lecture de deux premières valeurs successives va donner un 0 et un 1, il est alors impossible d'être dans le cas d'une suite constante, la suite est équilibrée. Dans la situation défavorable, les valeurs sont regroupées. La moitié des lectures donnera 0 et l'autre moitié 1. Il faudra alors lire la moitié des valeurs, soit $N/2$ pour ensuite tomber sur l'autre partie de la séquence et démontrer que nous sommes dans le cas équilibré.

En conclusion, le nombre de tests nécessaires pour savoir quel type de série est présenté varie entre 2 et $N/2 + 1$, dans le cas d'un algorithme classique.

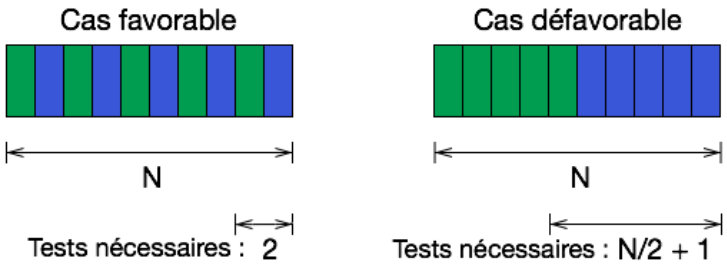

ILLUSTRATION 3.1 – Cas favorables et défavorables du problème.

L'algorithme de Deutsch-Jozsa est quant à lui capable de donner la réponse avec un seul test. Il est ainsi historiquement le premier algorithme quantique plus rapide que sont pendant classic. Il ne présente néanmoins pas de réelle application pratique, contrairement à celui de Shor.

3.2 L'algorithme de Shor

Cet algorithme pour le nom de son créateur : Peter Shor, actuellement professeur de mathématiques au prestigieux Massachusetts Institute of Technology. P. Shor est également connu pour ses travaux sur les circuits de correction d'erreurs quantiques.

ILLUSTRATION 3.2 – Peter Shor

Cet algorithme peut être utilisé pour trouver la décomposition d'un nombre en produit de facteurs de nombres premiers. Il est à noter que comme les autres algorithmes quantiques, il ne donne pas une réponse certaine à 100 %, mais seulement une réponse hautement probable. Plusieurs itérations de l'algorithme permettent de réduire l'incertitude jusqu'à obtenir un résultat que l'on peut considérer comme suffisamment exacte pour être exploitable.

Il fut le premier exemple concret démontrant un avantage d'efficacité conséquent d'un algorithme quantique sur son équivalent classique. Il permit également de mettre en évidence que certaines astuces mathématiques permettent de contourner le grand défaut du parallélisme quantique : un seul résultat lisible par exécution. Il démontra aussi que l'impact de la décohérence, sur le résultat, peut être réduit au niveau de l'algorithme. Ce sont ces raisons, et les implications en cryptographie, qui ont entraîné un regain d'intérêt pour le calcul quantique dès la publication des travaux de Shor.

3.2.1 Calcul de la période d'une fonction

Il est souvent entendu que l'algorithme de Shor consiste en la factorisation d'un nombre en produits de facteurs premiers. Ceci n'est pas tout à fait exact. En effet, la factorisation est une application directe de cet algorithme et non sa raison d'être. « L'algorithme de Shor (1994) permet ainsi de déterminer la période d'une fonction beaucoup plus vite que classiquement. » [Vio06].

Une fonction $f(x)$ est dite périodique si ses valeurs se répètent de façon cyclique. Il existe alors un réel r, positif et non nul, le plus petit possible appelé période de la fonction. Pour toute valeur de x, on obtient alors $f(x) = f(x + r)$.

La découverte de Shor est surtout connue parce qu'elle n'est pas seulement purement théorique, mais parce qu'elle possède aussi des applications pratiques. En effet, la connaissance de cette période r d'une fonction peut ensuite être utilisée pour en déduire d'autres éléments. La décomposition d'un nombre en un produit de facteurs premiers est un cas où cet algorithme peut être utilisé.

L'idée derrière l'algorithme de Shor est de ne pas chercher une valeur exacte, mais d'essayer de trouver une valeur suffisamment fiable pour être exploitée. Ceci peut être rapproché

au problème du voyageur de commerce [1]. Il est ainsi parfois plus intéressant d'obtenir rapidement un résultat approximé que d'attendre pour avoir la réponse parfaite. Pour factoriser un nombre en un produit de facteurs premiers, l'algorithme de Shor sert à accélérer une partie d'un algorithme classique. Cette optimisation permet de passer d'une complexité dite exponentielle à une dite polynomiale. Ceci signifie que le temps de calcul nécessaire en fonction de la taille du nombre croît moins vite pour la version optimisée par Shor que pour une version 100 % classique. Néanmoins ce gain d'efficacité n'est pas très visible pour de petits nombres, voir illustration 3.3.

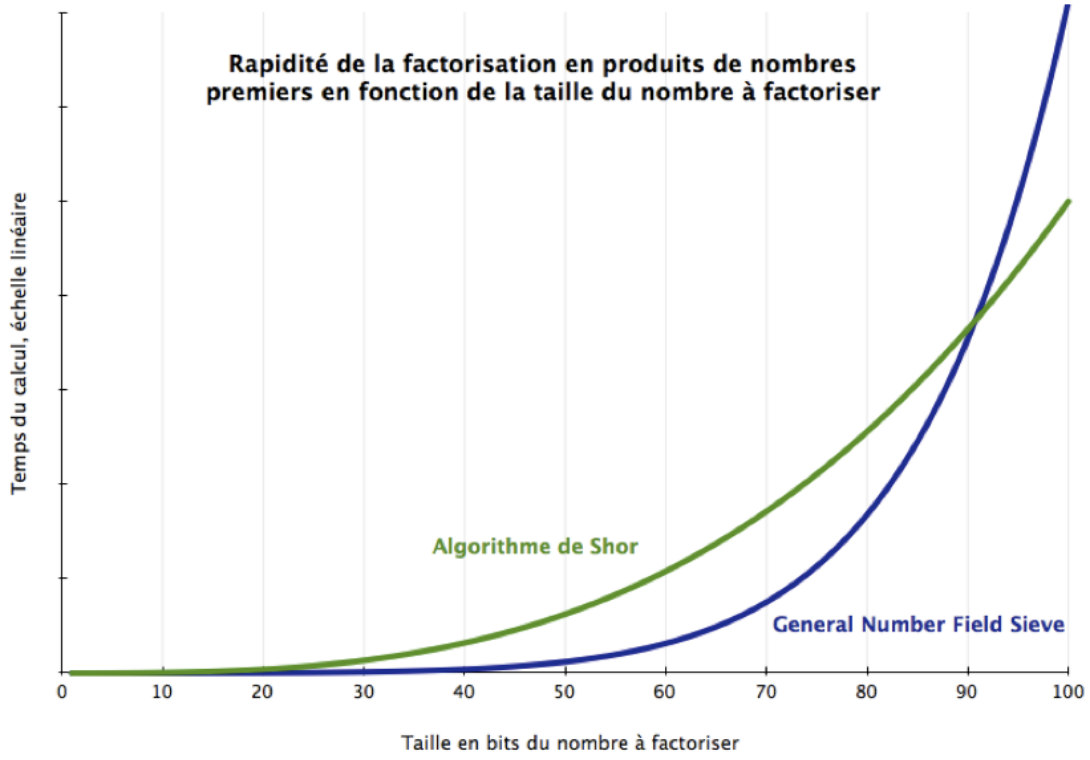

ILLUSTRATION 3.3 – Vitesse pour la factorisation d'un nombre de 100 bits et moins.

Ce n'est qu'à partir de nombres d'une taille supérieure à 90 bits que l'optimisation par l'algorithme de Shor devient réellement intéressante pour la factorisation des nombres, voir illustration 3.4.

Ainsi s'il est actuellement très long de factoriser un nombre produit de deux facteurs premiers de grande taille, avec l'algorithme de Shor, le temps devient raisonnable. Les deux illustrations présentées n'indiquent pas de façon exacte la durée du calcul en fonction de la taille du nombre. Elles représentent néanmoins de façon fidèle l'augmentation de ce temps de calcul. En effet, les courbes ont été tracées à l'aide de la complexité des algorithmes respectifs, ce qui en fait de très bons indicateurs pour leur efficacité relative.

1. Un commercial doit optimiser son trajet pour visiter toutes les villes dans le laps de temps le plus court possible

3.2.2 Utilisation en cryptographie

C'est cette difficulté à factoriser un nombre en produit de facteurs premiers qui est à la base de nombre de systèmes de cryptages. Ceux-ci, dits asymétriques ou à clefs publiques, comme le RSA utilisent pour clef un produit de nombres premiers (clefs de 1 024 bits minimum pour le RSA). Retrouver les nombres premiers permet de craquer le code, mais l'opération est tellement longue que l'on peut considérer que le système est sûr.

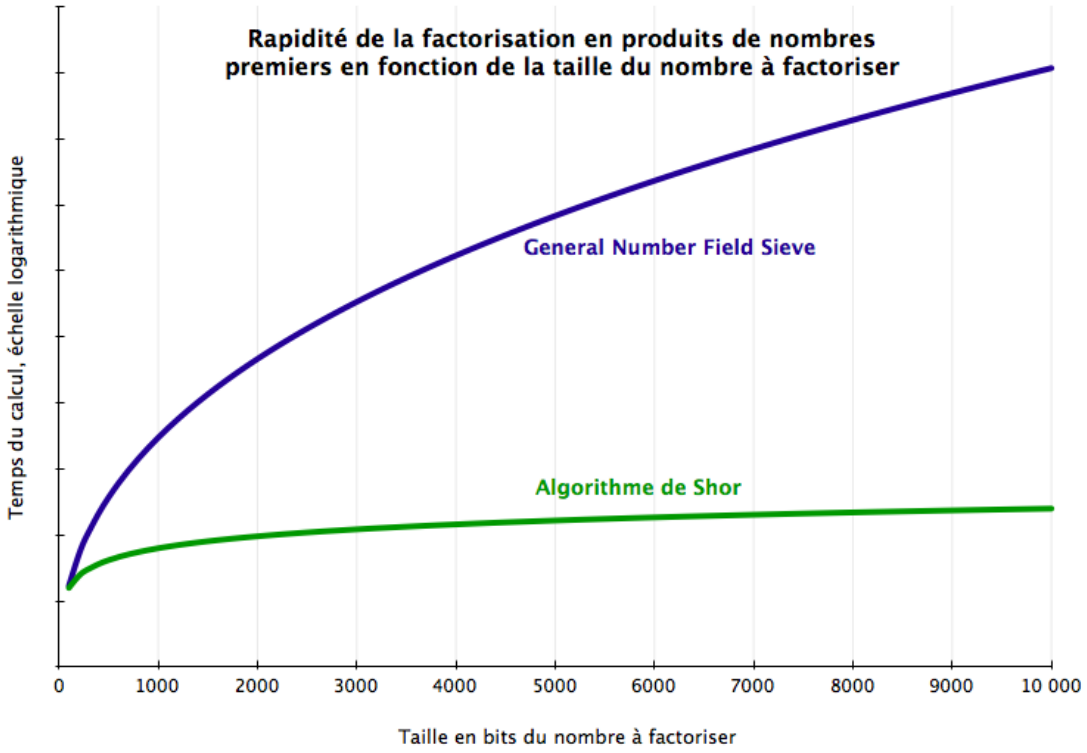

ILLUSTRATION 3.4 – Vitesse pour la factorisation d'un nombre de 100 bits et plus.

Sur l'illustration 3.4 l'axe des ordonnées utilise une échelle logarithmique. L'implémentation de l'algorithme de Shor sur un ordinateur quantique pleinement fonctionnel permettrait de briser ces codes dans un temps relativement raisonnable, rendant tous ces systèmes de cryptage caducs.

Cette constatation a entraîné un regain d'intérêt des militaires et industriels pour le calcul quantique.

> « It wasn't until 1994, when Peter Shor surprised the world by describing a polynomial time quantum algorithm for factoring integers [Shor 1994 ; Shor 1997], that the field of quantum computing came into its own. » [RP00]

3.3 L'algorithme de recherche de Grover

Tout comme Peter Shor, Lov Grover travaillait chez AT&T, et plus spécifiquement aux laboratoires Bells lorsqu'il inventa son algorithme en 1996.

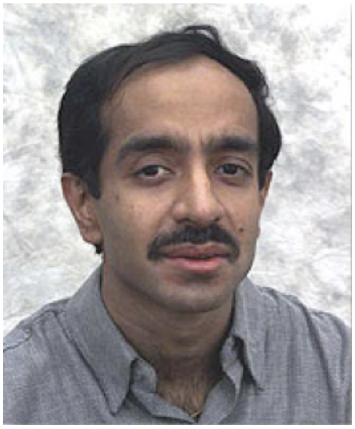

ILLUSTRATION 3.5 – Lov Grover

Supposons que nous recherchons un enregistrement dans une base de données non triées. Nous disposons d'une fonction permettant de savoir si l'enregistrement lu est celui recherché ou non.

Statistiquement, pour avoir 50 % de chances de trouver l'enregistrement parmi les N présents, il faut avoir testé $N/2$ enregistrements existants. L'algorithme de Grover permet lui d'avoir une très forte probabilité d'avoir trouvé l'enregistrement avec « seulement » $(\pi/4)\sqrt{N}$ itérations [2]. Le gain de vitesse par rapport à une recherche classique est polynomial. Si cette optimisation n'est pas aussi marquée que celle de l'algorithme de Shor, elle reste néanmoins très intéressante. De plus l'accélération des recherches peut être perçue même sur des bases de données d'une dizaine d'enregistrements, voir illustration 3.6. Ceci permet de ne pas avoir de contrainte de taille minimum avant de pouvoir utiliser cet algorithme, là où celui de Shor nécessitait d'avoir un nombre d'au moins 90 qubits.

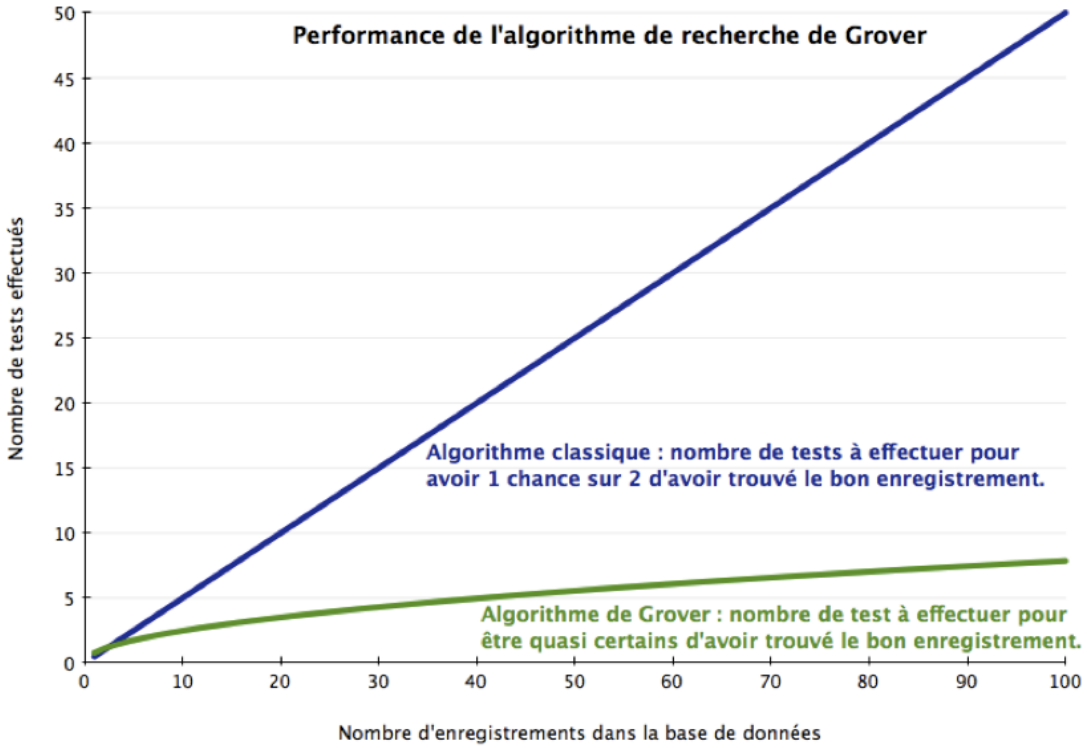

ILLUSTRATION 3.6 – Vitesse de recherche en fonction de la taille d'une base de données.

2. Il ne s'agit pas ici d'une moyenne mais du nombre réel d'itérations à réaliser. Ce n'est qu'avec le respect de ce nombre de cycles qu'il est possible d'obtenir une forte probabilité de trouver le bon enregistrement

Sur le graphique 3.6 l'axe des abscisses représente le nombre d'éléments dans la base de données. L'axe des ordonnées correspond aux nombres de tests effectués. La couleur bleue est utilisée pour indiquer l'évolution de la durée d'exécution de l'algorithmique classique. La droite représente le nombre de tests effectués, en fonction du nombre d'enregistrements, pour avoir 50 % de chances d'avoir retrouvé la donnée escomptée. Le vert représente le nombre de tests effectués pour être quasi-certains d'avoir trouvé la bonne valeur avec l'algorithme de Grover. Ce graphique est surtout utile pour démontrer que l'algorithme de Grover devient d'autant plus intéressant que la taille de la base de données augmente.

Pour avoir ces performances, l'approche est différente de celle utilisée par Shor. Plutôt que de déduire une information de plusieurs lectures successives, il s'agit ici de réaliser un traitement dont le but est d'augmenter la probabilité que la donnée qui sera lue à la sortie soit celle recherchée.

3.3.1 Les limitations de l'algorithme de recherche de Grover

L'algorithme de Grover n'est intéressant que dans le cas où la base de données est dite non triée. Ceci signifie que les enregistrements ne sont pas rangés, ni ne possèdent d'index. Dans le cas contraire, l'utilisation de méthodes, telles que la dichotomie ou les arbres binaires de recherches, permet de réduire grandement le nombre moyen de tests à réaliser, avec un algorithme quantique, pour trouver la donnée recherchée. Or la méthode proposée par Grover n'est pas capable d'utiliser le fait que la base de données est triée, il nécessite le même nombre d'itérations dans les deux cas.

Ainsi, les méthodes classiques devenant plus efficaces, l'utilisation de l'algorithme de Grover perd de l'intérêt pour les bases de données triées. Le gain de vitesse diminue.

De plus, l'algorithme de Grover perd aussi de l'intérêt lorsqu'il existe plusieurs données qui répondent aux critères demandés.

Chapitre 4

Les processeurs quantiques

Si le calcul à l'échelle quantique est possible au niveau algorithmique, son implémentation est une autre histoire. Plusieurs voies de recherches sont actuellement explorées pour essayer de mettre au point un processeur quantique. Si certaines reposent sur l'utilisation d'éléments déjà quantiques, d'autres préfèrent partir d'éléments macroscopiques et essayer d'y faire apparaître des phénomènes quantiques.

Il ne s'agit pas ici de rentrer en détail dans les différentes techniques envisagées, mais de donner un aperçu du fonctionnement de certaines d'entre elles et des difficultés qu'elles rencontrent.

4.1 La résonance magnétique nucléaire

Cette technique reste officiellement celle qui a donné les meilleurs résultats. Elle n'a pourtant presque pas évolué depuis 2001. Elle est aussi connue sous son sigle RMN, ou NMR en anglais.

4.1.1 Présentation de la méthode

La résonance magnétique nucléaire a été inventée en 1939 par le physicien américain Isaac Rabi. Elle à donnée par la suite l'Imagerie à Résonance Magnétique Nucléaire, connue sous le nom d'IRM. Lorsque les noyaux des atomes sont soumis à un champ magnétique, ils absorbent puis réémettent cette énergie à une fréquence de résonance qui leur est propre et peut être mesurée.

Le dispositif de RMN :

Un tube contenant des molécules est placé entre une série d'aimants :
- des aimants permanents qui assurent un champ magnétique constant

– des électroaimants situés perpendiculairement aux premiers et qui génèrent des impulsions magnétiques

Ce dispositif permet de modifier et de lire une propriété purement quantique : le *spin* des atomes présents dans la fiole. Le spin correspond à la rotation des particules sur elles-mêmes et est responsable des propriétés magnétiques des matériaux.

Le spin peut être *parallèle* ou *antiparallèle*. En temps normal, il existe autant de spins de l'un et de l'autre dans un fluide, mais le champ magnétique appliqué peut être utilisé pour modifier l'état du spin, créant ainsi un léger déséquilibre qui peut être mesuré.

Dans cette méthode, les qubits sont les atomes même de la molécule, ce qui implique qu'il existe autant de processeurs quantiques que de molécules présentes dans l'expérience. La multiplication de ces processeurs permet une meilleure mesure.

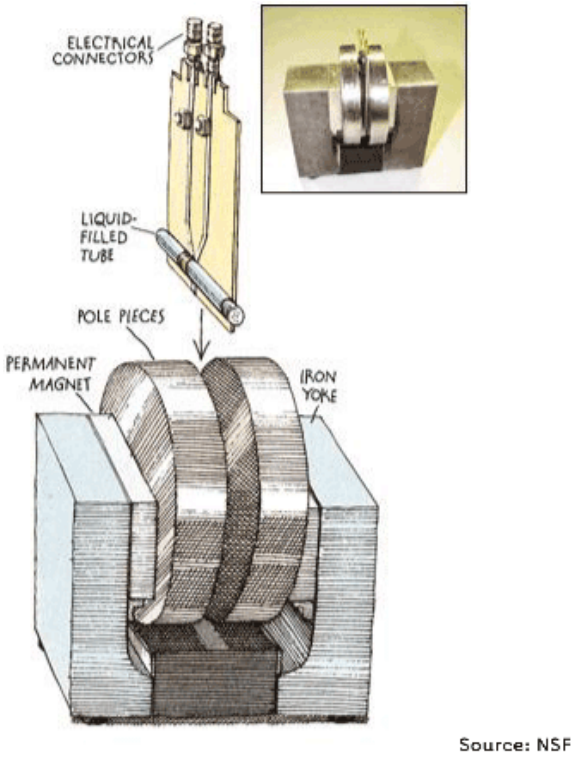

ILLUSTRATION 4.1 – RMN

La réalisation d'un calcul commence par l'initialisation des molécules dans un état de départ, puis par une série d'impulsion magnétique correspondant aux différentes étapes de l'algorithme. Une fois le "programme" terminé, le résultat peut être lu.

4.2 Le travail d'Isaac L. Chuang

C'est avec cette technique qu'a été réalisé le premier processeur quantique en 1998, dans les laboratoires d'IBM. L'équipe d'Isaac L. Chuang [VYC00], également professeur au MIT depuis l'an 2000, a en effet réussi à réaliser un processeur à deux qubits et utilisant comme support des molécules de chloroforme.

ILLUSTRATION 4.2 – Isaac Chuang

Un an plus tard, cette technique permettait d'atteindre 3 qubits, puis 5 en l'an 2000. Sur ces deux modèles, ils ont réussi à utiliser l'algorithme de recherche de Grover, vu plus tard dans ce document.

Toujours en utilisant cette technique, la même équipe a réussi en 2001 à faire tourner l'algorithme de Shor, que nous verrons

également par la suite. Ils ont ainsi pu “calculer” que le nombre 15 est le produit de 3 et 5, deux nombres premiers. Le processeur utilisé disposait alors de 7 qubits. Cette expérience reste encore à ce jour la plus grande réalisation dans ce domaine.

4.3 Les défauts de cette technique

Cette technique semblait très prometteuse et est celle qui a, jusqu’à présent, donné les meilleurs résultats, comme l’a rappelé l’article dans le magazine du CNRS, 10 ans plus tard. « *At present, the best computing feat performed with qubits is that of Isaac Chuang at the Massachusetts Institute of Technology* » [CNR11].

Le problème est qu’en raison du support, les atomes présents dans des molécules, le nombre maximal de qubits dans ce type d’ordinateur peut difficilement dépasser la dizaine.

Un autre défaut de cette technique est la durée de vie du processeur qui ne dépassait pas quelques minutes.

Suite à ce constat I. Chuang à décider de se tourner vers une autre voie de recherche : l’approche des ions piégés. Mais avant de voir celle-ci, il est intéressant d’étudier un principe souvent associé à ceux-ci : les qubits optiques.

4.4 Le qubit optique

Par l’utilisation de lasers venant bombarder des atomes ou ions isolés, il devient possible de transformer ces derniers en qubits. Ces techniques basées sur l’optique, et étudiées, entre autre, par l’Institut d’Optique d’Orsay, permettent à la fois d’isoler les atomes ou ions, de manipuler leur état quantique, et de permettre une lecture.

> « *Notre groupe a développé une expertise dans le piégeage d’atomes neutres dans des pinces dipolaires optiques. Nous avons montré que nous pouvons piéger dans une pince optique un atomes unique, dans un volume de l’ordre du micron cube, pour des durées de l’ordre de la seconde. Nous avons également montré que nous savons piéger individuellement plusieurs atomes à des positions contrôlées à mieux qu’un micron près. Cela permet d’envisager la réalisation d’un ensemble d’atomes adressables individuellement par des moyens optiques, permettant le stockage de bits quantiques (qubits), c’est-à-dire un “registre quantique”. Nous avons également montré que nous pouvons produire des photons uniques émis à la demande par un unique atome piégé. Une telle source de photon uniques constitue un dispositif fondamental pour l’information quantique, car elle permet de convertir un qubit “stationnaire” (bit quantique d’information quantique stocké dans un atome) en qubit “volant” (bit quantique d’information stocké dans un photon).* » [Gra]

Outre l'Institut d'Optique, d'autres laboratoires explorent ces possibilités. Notamment celui de physique de l'Université de Bristol [1], en Grande Bretagne. Celui-ci étudie également l'optique quantique pour une utilisation en cryptographie, pour une transmission non-interceptable d'informations.

Cette technologie, couplée à celle des ions piégés, a déjà permis de réaliser des portes logiques quantiques.

> « *Partant de systèmes très quantiques comme des spins nucléaires (à la base de la résonance magnétique nucléaire, la RMN), ou d'ions piégés dans des cavités (optique quantique), plusieurs groupes ont déjà construit des portes logiques élémentaires* ». [Est05]

4.5 La technique des ions piégés

Comme il l'est vu au collège puis au lycée, un ion est un atome, ou une molécule, dont la charge électrique est non neutre. Ceci signifie que le nombre d'électrons est soit inférieur, on parle alors de cations, soit supérieur, pour les anions, au nombre de protons. Ceci explique une des caractéristiques des ions, qui est qu'ils sont attirés par les champs magnétiques.

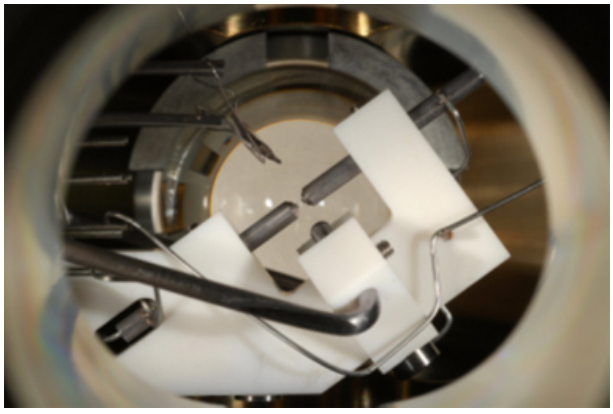

ILLUSTRATION 4.3 – Piège pour un ion de strontium.

Cette caractéristique permet d'en isoler un petit nombre au sein d'une cavité sous vide. Ils sont alors refroidis à l'aide de lasers, utilisés pour forcer le niveau d'énergie des électrons à redescendre par émission de photons, les mettant dans l'état $|0\rangle$. Chacun de ces ions isolés représente alors un qubit. Ils sont alors "liés" les uns aux autres, toujours à l'aide de lasers, permettant alors de créer un processeur avec l'ensemble de ces ions. « *By applying lasers that apply a force depending upon the qubit state, multiple ions can be entangled through their collective motion.* » [SHOM06]. Cette liaison des qubits est réalisée avec la même procédure que celle employée pour réaliser la première "téléportation". Il a, en effet, été possible de lier deux photons de façon à ce qu'une transformation de l'état de l'un entraîne la même transformation

1. http ://www.phy.bris.ac.uk/groups/cqp/research.html

sur le second instantanément, tout le terme de téléportation, dans le sens de “transfert immédiat”.

L’avantage de cette technique par rapport aux autres est la possibilité de modifier le nombre de qubits présents dans le processeur. Il est en effet possible de préparer un nombre x de pièges à ions et de faire varier le nombre d’ions effectivement piégés entre 0 et x, modifiant ainsi le nombre de qubits du processeur.

Fin 2005, l’équipe de Chris Monroe [SHOM06] de l’Université du Maryland a réussi à créer un tel piège.

4.6 D-Wave

D-Wave Systems, Inc. est une compagnie canadienne qui fait la controverse depuis plusieurs années. En 2007, cette compagnie a annoncé la mise au point du premier microprocesseur quantique fiable, avec 16 qubits. Celui-ci serait construit comme un circuit électronique, utilisant un supra-conducteur : le niobium [Col07]. Certains des scientifiques travaillant sur les processeurs quantiques ne sont pas convaincus que la solution proposée par D-Wave est réellement quantique. Interrogé sur l’état de l’art lors de notre entretien, le docteur Daniel Esteve n’a fait nulle mention de D-Wave, qui pourtant utiliserait le même principe que le groupe Quantronics : des circuits supraconducteurs. Un scientifique en informatique de l’Université Californienne de Santa Barbara, Wim van Dam, à ainsi exprimé les doutes quant à la valeur de la présentation de D-Wave.

> « *In February 2007, D-Wave created a splash when its 16-qubit machine solved several puzzles—although none that a conventional computer couldn’t handle—such as figuring out how to seat guests around a table so that people who dislike each other do not end up side by side. However, “people had serious doubts that this was a true quantum computer,” says Wim van Dam, a theoretical computer scientist at UCSB.* » [Cho11]

D-Wave a annoncé le 25 mai 2011 avoir vendu son premier ordinateur quantique, à une filiale de Lockheed Martin [DW]. Le processeur ferait 128 qubits et serait composé de 8 cellules de 16 qubits. Le doute subsiste, moins sur le fait que des phénomènes quantiques soient présents, que sur le fait que les 128 qubits soient vraiment liés ensembles. La cohérence serait ainsi perdue trop vite pour que l’on puisse réellement parler d’un processeur quantique.

> « *But it’s possible that D-Wave’s qubits lose coherence very quickly to act more or less independently but nonetheless tunnel to their collective ground state. And in that case, the computer can’t hope to be any more efficient than a regular one, van Dam says.* » [Cho11]

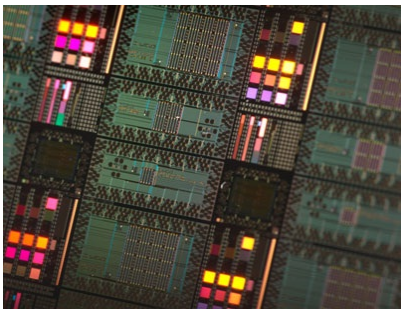

ILLUSTRATION 4.4 – Le processeur de D-Wave

4.7 Les circuits supraconducteurs

Une des voies de recherches envisagées est l'usage de circuits à base de supraconducteurs. La supraconductivité est un phénomène obtenu sur certains matériaux refroidit à de très basses températures, proches du zéro absolu, c'est-à-dire à peines supérieures à -273,15 °C. Cette technique est étudiée notamment en France au groupe Quantronics, en Allemagne à l'université de technologie de Delft et aux États Unis dans les universités de Yale et Santa Barbara.

4.7.1 Les propriétés des supraconducteurs

Les supraconducteurs sont surtout connus pour posséder une résistance électrique quasi-nulle. Celle-ci implique qu'il n'existe pas de dissipation d'énergie par effet joule. Ainsi l'énergie mise dans un matériau supraconducteur reste constante.

Une seconde propriété moins connue des supraconducteurs est appelée l'effet Meissner. Elle se caractérise par l'exclusion des champs magnétiques. Alors qu'ils pénétreraient dans un conducteur classique et causeraient des perturbations, ils sont repoussés autour d'un supraconducteur. Ce phénomène explique qu'un aimant se met à léviter lorsqu'il est placé au-dessus d'un matériau supraconducteur.

Ces deux propriétés sont intéressantes pour la réalisation de qubits. En effet, un matériau supraconducteur placé dans un état de superposition y reste car il n'y a pas de perte d'énergie, ni de perturbations induites par les champs magnétiques extérieurs.

4.7.2 Le quantronium

Bien que maintenant obsolète et remplacé par de meilleurs circuits, le quantronium est un bon exemple pour comprendre le fonctionnement de ces circuits.

Le quantronium est le nom du circuit sur lequel travaillait le groupe quantronics en 2002. Il est créé à l'aide d'une boucle supraconductrice coupée par trois éléments appelés jonctions Josephson. Une jonction Josephson est obtenue en séparant des électrodes, supraconductrices, par un isolant électrique qui soit suffisamment mince pour laisser passer une paire d'électrons.

Il faut en effet savoir que, dans un supraconducteur, les électrons qui le parcourent sont toujours liés deux à deux. On parle de paires de Cooper.

Sur les trois jonctions, deux servent à créer une zone isolée suffisamment petite pour que seuls deux électrons puissent s'y trouver. Cette zone est le qubit proprement dit. Les deux jonctions qui délimitent le qubit sont plus petites que la troisième jonction dont le rôle est de permettre la lecture de l'état du qubit.

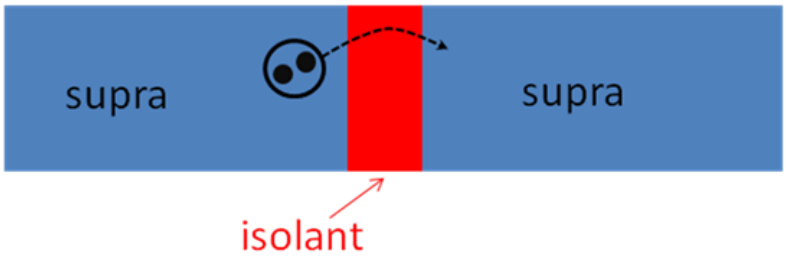

ILLUSTRATION 4.5 – Jonction Josephson

L'utilisation de matériaux supraconducteurs permet à la fois l'obtention d'un qubit sous la forme de deux électrons isolés, mais aussi de garantir une assez bonne protection face à la décohérence liée au rayonnement thermique.

> « *Superconducting quantum circuits have been proposed as qubits for developing quantum computation. The goal is to use superconducting quantum circuits to model the measurement process, understand the sources of decoherence, and to develop scalable algorithms.* » [OLL+02]

4.8 Les principaux problèmes

4.8.1 La durée de vie du processeur

La recherche sur les processeurs quantiques est encore loin d'être terminée. Malgré quelques réussites dans ce domaine, il n'est pas encore certain qu'un ordinateur quantique fiable et utilisable puisse être fabriqué. E. Rieffel et W. Polak, deux scientifiques qui s'intéressent au calcul quantique, ce problème est le plus important à se poser. « *Perhaps the biggest open question is wether useful quantum computers can be build.* » [RP00]. En effet même les prototypes d'IBM, pourtant les plus aboutis, ne peuvent fonctionner qu'un court instant.

Le principal problème pour la durée de vie est le problème dit de la décohérence. Il s'agit d'un phénomène ou un élément obéissant aux règles de la physique quantique finit par basculer dans le domaine de la physique classique. La raison étant la difficulté d'isoler suffisamment le processeur pour empêcher l'environnement d'interagir avec lui. Rieffel et Polak indiquent d'ailleurs que les scientifiques ont longtemps pensé que ce phénomène à lui seul pourrait empêcher la réalisation d'un ordinateur quantique.

> « *The greatest problem for building quantum computers is decoherence, the distortion of the quantum state due to interaction with the environment. For some time it was feared that quantum computers could not be built because it would be impossible to isolate them sufficiently from the external environment.* » [RP00]

Les réussites au début du 21ème siècle ont montrés que le problème de la faisabilité n'est plus, reste encore celui de l'utilisabilité.

4.8.2 Le problème de l'échelle

Plusieurs voies de recherches sont actuellement poursuivies mais elles se confrontent toutes à l'autre grand problème : celui de l'échelle des processeurs. Il ne s'agit pas d'un problème de taille du processeur, mais du nombre de qubits présents.

> « *There are a number of proposals for building quantum computers using ion traps, nuclear magnetic resonance (NMR), optical and solid state techniques. All of the current proposals have scaling problems, so that a breakthrough will be needed to go beyond tens of qubits to hundreds of qubits. While both optical and solid state techniques show promise, NMR and ion trap technologies are the most advanced so far.* » [RP00]

En effet, contrairement au cas de l'informatique classique, la performance d'un processeur quantique se mesure principalement à la taille des nombres qu'il peut traiter (en bits pour le premier et qubits pour le second). Pour des nombres de petites tailles, c'est-à-dire d'une dizaine de bits, un calculateur classique est plus performant qu'un calculateur quantique. Mais au-delà d'une certaine taille la situation s'inverse, comme l'a montré l'algorithme de Shor et l'ont rappelé P. Ribiero et F. Nguyen dans un rapport qu'ils ont rédigés suite à un stage de fin d'étude au CEA.

> « *The advantage of quantum algorithms is only achieved when a large number of qubits can be reliably manipulated ...* » [Rib05]

En effet, l'algorithme de Shor pour la factorisation des nombres se révèlent exponentiellement plus rapide que les algorithmes classiques pour des nombres de plus de 90 bits de large. Il faut aussi savoir qu'il est difficile de réaliser des opérations dans un processeur quantique sur des nombres de largeur supplémentaire à celle du processeur. Dans un ordinateur classique, cela est possible grâce à la possibilité de conserver les résultats intermédiaires, comme la retenue des additions. Mais comme nous l'avons déjà vu, il n'est pas possible de réaliser une copie d'un état quantique, il ne peut donc pas exister de valeurs intermédiaires, tous les traitements doivent être effectués d'un bloc. De plus, augmenter la largeur d'un processeur classique n'augmente pas sa vitesse, sauf si cela permet de réaliser en une seule fois une opération qui nécessitait des valeurs intermédiaires et par là même plusieurs cycles. Par exemple, être passé d'une architecture 32 bits à 64 bits n'a pas accéléré la vitesse des calculs sur les entiers 32 bits. Par contre, elle a

permis d'avoir des calculs sur les entiers 64 bits en une seule opération. De l'autre côté, dans le cas des processeurs quantiques, la vitesse dépend de la taille. Réaliser une opération sur x qubits revient à réaliser la même opération dans un ordinateur classique. Augmenter de 1 qubit la largeur du processeur revient à doubler la performance.

Chapitre 5

Description des améliorations

Avant de pouvoir être en mesure de proposer des évolutions, il nous fallait commencer par connaître l'état de l'art. Ceci pour cerner suffisamment bien le sujet afin d'être en mesure de voir les manques et points à améliorer. Après avoir eu un premier aperçu de la question, le choix des personnes à interviewer a été déterminant. Elles ont permis à la fois d'approfondir la compréhension de la problématique, et de confirmer la pertinence de l'axe d'amélioration envisagé à l'époque.

La première personne rencontrée, le Docteur Daniel Esteve, a ainsi pu me donner des renseignements sur la partie matérielle de la problématique. Bien qu'il soit surtout spécialisé sur les processeurs quantiques à base de supraconducteurs, ses explications sur les contraintes auxquelles doivent répondre un processeur quantique furent très utiles. Le compte rendu de cet entretien peut être vu dans les annexes, à partir de la page 57.

Ensuite, l'interview du Docteur Julia Kempe, focalisée sur la partie algorithme, a surtout donné des indications sur la capacité à exploiter les processeurs quantiques. En effet, en réaliser un et savoir l'utiliser restent deux choses différentes. La retranscription de cette interview est consultable dans les annexes, à partir de la page 62.

Ces deux entretiens ont permis de couvrir tous les aspects de l'informatique quantique, le *hardware* et le *software*. Ils constituent ainsi une base solide sur laquelle s'appuyer pour proposer des évolutions.

5.1 Améliorations souhaitables

Les précédentes parties ont permis de mettre en évidence les principaux obstacles actuellement rencontrés au niveau matériel, c'est-à-dire :

- la décohérence,
- le temps d'utilisation réduit,
- le faible nombre de qubits des prototypes de processeurs quantiques réalisés,
- le nombre encore réduit d'algorithmes.

Comme le Docteur Daniel Esteve l'a indiqué lors de notre entretien, augmenter le temps de cohérence permettrait à lui seul d'augmenter le temps d'utilisation et de permettre la construction de prototypes avec plus de qubits. De ce fait, il semble que ce soit la principale amélioration à vouloir actuellement, pour la réalisation d'un processeur quantique.

Il existe néanmoins un autre axe d'amélioration qui devrait mériter notre attention. Cet aspect ne concerne pas la réalisation d'un ordinateur quantique, mais son utilisation. La conception et la réalisation d'un processeur quantique restent en effet trop complexe pour être vraiment appréhendée par un étudiant en informatique. Néanmoins, réfléchir à des moyens d'intégrer un tel processeur au sein d'une architecture "classique" reste concevable.

C'est pour cela qu'il faudrait commencer à réfléchir à comment la technologie quantique pourrait être utilisée demain. Il faut, en effet, garder à l'esprit qu'informatique quantique et classique sont trop différentes pour que la première puisse vraiment remplacer la seconde. D'un autre côté, cela signifie aussi qu'elles pourraient être complémentaires l'une de l'autre.

Il nous faut réfléchir à un moyen d'arriver à exploiter la technologie quantique dans les futures générations d'ordinateurs.

5.2 Recherche d'axes d'améliorations

Nous ne pouvons pas encore prévoir ce que sera vraiment l'informatique quantique, nous ne savons pas quelle technologie permettra de la construire. À partir de ce moment-là, nous ne pouvons pas avoir une vision vraiment claire du futur. C'est pourquoi la meilleure façon pour essayer d'imaginer une solution est de s'inspirer du passé. Nous pouvons ainsi nous baser sur l'apparition passée d'une technologie pour voir ce qu'elle à améliorer.

5.2.1 La similitude avec les superordinateurs

Pour notre recherche de solutions possibles, nous pouvons nous inspirer du calcul HPC [1]. En effet à partir des années 1960 est apparu un progrès technologique connu sous le nom de superordinateurs. Sur bien des aspects, ils présentent par rapport aux ordinateurs de bureaux le même décalage qu'il existerait avec les ordinateurs quantiques.

La première similitude est qu'ils sont basés sur le parallélisme. En effet les superordinateurs utilisaient au départ des processeurs vectoriels [2] avant d'évoluer pour utiliser plusieurs processeurs. La dernière génération de superordinateurs est basée sur la mise en réseau d'ordinateurs. Dans les deux derniers cas, on parle de calcul distribué.

1. High Perfomance Computing, Calcul haute performance
2. Un processeur vectoriel réalise simultanément une même opération sur plusieurs jeux de données.

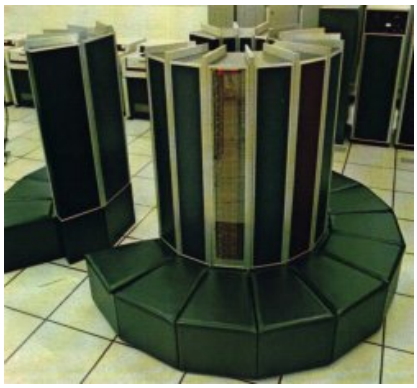

ILLUSTRATION 5.1 – Le cray 1 est un des plus célèbres superordinateurs. Il est reconnaissable à sa forme en arc de cercle. Il utilise un unique processeur vectoriel 64 bits.

De plus, tout comme les ordinateurs quantiques, si les superordinateurs sont très efficaces pour un certain nombre de tâches, ils le sont beaucoup moins pour les autres tâches. Ceci explique que les superordinateurs restent assez peu répandus et sont surtout situés dans de grands centres de recherche.

Il se trouve que nos ordinateurs de bureaux bénéficient aujourd'hui de certains principes développés à l'origine pour les superordinateurs. Ces gains se retrouvent aussi bien dans les microprocesseurs que dans l'architecture des ordinateurs. Ils se retrouvent sous la forme :

- des unités de calcul vectoriel, SIMD [3], présentent dans les processeurs, (sortie en 1999 du SSE sur les processeurs Intel et de l'Altivec sur les Power PC)
- des processeurs à plusieurs coeurs,
- des ordinateurs multi-processeurs,
- des cartes graphiques, leur fonctionnement repose justement sur le parallélisme.

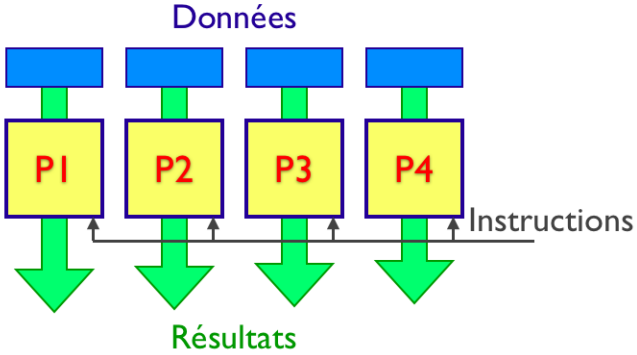

ILLUSTRATION 5.2 – Exemple d'architecture SIMD, le même calcul est effectué sur 4 jeux de données différentes

3. Single Instruction Multiple Data

5.2.2 Comment exploiter cette similitude

Cette similitude entre ordinateurs quantiques et superordinateurs va nous être utile pour trouver des axes possibles afin de proposer une solution pour mieux exploiter cette technologie future pour les microprocesseurs de demain.

Après avoir étudié les bases des ordinateurs quantiques, il semble assez peu concevable de travailler avec un ordinateur qui soit purement quantique. L'informatique traditionnelle est en effet beaucoup trop ancrée dans notre quotidien pour pouvoir nous en passer. La factorisation des nombres premiers par l'algorithme de Shor, que nous avons vu précédemment, n'utilise-t-elle pas de base un algorithme classique ? Tout comme les superordinateurs peuvent proposer des performances de très loin supérieures à nos ordinateurs de bureaux, ils n'ont pas remplacé ces derniers.

De plus, à l'heure actuelle, les prototypes de processeurs quantiques ont besoin d'un système de contrôle classique pour fonctionner. Interrogé sur la question de réaliser un ordinateur purement quantique, la réponse du Docteur Esteve fut « *Les qubits ne sont intéressants que pour des phases où le calcul peut bénéficier du gain exponentiel de certains algorithmes quantiques.* ». Essayer de faire disparaître la technologie classique ne semble, en définitive, pas être une bonne idée.

Ainsi, ce sur quoi nous devons réfléchir n'est pas comment remplacer la technologie actuelle par celle quantique. Il s'agit en fait de savoir comment exploiter celle-ci afin de permettre une amélioration de la technologie actuelle. Il paraît également concevable d'imaginer une informatique qui continuerait à être basée sur des processeurs classiques, mais serait capable de sous-traiter certains calculs à l'informatique quantique.

5.3 Les axes retenus

5.3.1 Les deux axes retenus

Nous retiendrons deux grands axes de recherche pour l'exploitation des recherches en informatique quantique. Si le second repose sur l'utilisation du calcul quantique, le premier axe proposé repose sur une amélioration des capacités des processeurs actuels.

Il serait en effet intéressant de commencer par utiliser ces recherches afin de "blinder" les microprocesseurs. Une meilleure compréhension des phénomènes quantiques, notamment de la superposition, pourrait permettre de repousser légèrement la limite de la miniaturisation des composants. Ceci est déjà d'actualité comme l'a indiqué le Docteur Kempe dans une de ses réponses : « *Même s'il est vrai qu'en général on nous demande maintenant qu'est-ce qui peut être fait pour éviter les effets quantiques qui "pourrissent" les microprocesseurs. Pour cette question il est possible de donner quelques réponses.* », « *Ils verront comment procéder pour avoir de meilleurs microprocesseurs, mais je ne peux pas vraiment prédire comment ils seront.* ». Les

travaux sur la correction d'erreur quantique devraient notamment permettre d'améliorer la robustesse contre l'apparition de la superposition d'états.

Le second axe proposé est la réalisation d'unités de calculs utilisant la technologie quantique. Celles-ci resteraient plus que probablement pilotées par des ordinateurs classiques, et ne seraient destinées qu'à faire tourner des algorithmes quantiques vraiment plus efficaces que leurs pendants classiques.

5.3.2 La justification de ce choix

La première raison pour laquelle ces deux axes ont été retenus est parce qu'ils sont basés sur des concepts qui restent à notre portée. Ainsi, même en considérant que la technologie quantique est loin d'avoir été mise au point, il s'agit de choses que notre esprit permet déjà de concevoir. Ils restent en effet basés sur des technologies actuelles.

La seconde raison est qu'ils sont basés sur l'enseignement du passé. Ceci permet à ces propositions de rester réalistes et cohérentes avec l'évolution de l'informatique.

La troisième et dernière raison est qu'ils permettent de nous recentrer sur l'intitulé original du mémoire : les bénéfices de l'informatique quantique pour les microprocesseurs de demain.

5.4 Description détaillée

5.4.1 L'amélioration des processeurs actuels

Nous savons que dans la course à la miniaturisation des composants, nous finirons par atteindre une zone où les phénomènes quantiques commenceront à ne plus pouvoir être ignorés. Une fois entrée dans cette zone, la technologie actuelle des microprocesseurs ne pourra plus être utilisée. L'idée ici ne serait pas de repousser cette zone, cela n'est pas possible. L'idée serait d'être capable d'entrer dans cette zone, où phénomènes quantiques et classiques existent ensemble, plutôt que de devoir s'arrêter à la porte. Nous pourrions ainsi repousser légèrement la limite de la miniaturisation des composants.

Le principe de la correction d'erreurs quantiques semble tout indiqué pour cette tâche. Si nous devenons capables de lutter contre la décohérence, nous devrions aussi permettre de maintenir un système dans un état définit plutôt que dans une superposition d'état. En effet, lutter contre la décohérence signifie garder des valeurs de α et β constante dans l'équation $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, si l'un des coefficients est à 0 et l'autre vaut 1, alors nous pouvons maintenir des états $|0\rangle$ et $|1\rangle$. Le calcul classique redeviendrait alors possible à l'échelle quantique. Les recherches en informatique quantique servirait alors à améliorer les processeurs "classiques" de demain.

Néanmoins, ceci ne ferait que repousser légèrement la limite de la miniaturisation. En effet, la mise en place de la correction quantique nécessiterait d'utiliser des composants supplémentaires. L'espace gagné devant être en partie utilisé par des composants supplémentaires permettant au processeur de continuer à marcher, le gain de la miniaturisation deviendrait rapidement nul. De plus, si ceci permettrait d'augmenter les performances, cela n'améliorerait pas l'efficacité. L'utilisation de véritables processeurs quantiques deviendra alors incontournable pour pouvoir aller encore plus loin dans l'accélération des calculs.

5.4.2 La réalisation d'unités de calcul quantique

Ces unités ne seraient pas des ordinateurs à part entière, elles nécessiteraient d'être pilotées par un système de contrôle "classique". Un algorithme quantique et des données de travail leur seraient fournies et elles retourneraient un résultat. Ce résultat ne serait pas nécessairement exact, comme dans le cas des algorithmes de Shor et Grover, mais il aurait de très grandes probabilités de l'être.

Nous pourrions imaginer disposer de d'unités de calculs avec plusieurs processeurs. En effet, comme nous l'avons vu, un même calcul quantique peut avoir besoin d'être réalisé plusieurs fois au sein d'un algorithme. Ceci permettant de compenser le fait qu'un seul résultat puisse être lu à la fois. Comme l'a indiqué le Dr Esteve « *Mais lors de la lecture on ne peut accéder en général qu'à un seul des résultats. C'est pour cela que le parallélisme quantique n'est pas aisément exploitable.* ». Nous pourrions alors disposer de grandes unités de calculs incluant plusieurs processeurs quantiques, tous réalisant simultanément le même calcul. Ces unités pourraient alors réaliser chacune de ces étapes d'algorithme nécessitant plusieurs lectures en un temps relativement faible.

Nous pourrions aussi disposer d'unités de calculs plus petites, avec seulement une poignée de processeurs, voir un seul. Ces petites unités seraient alors plus facilement intégrables à côté d'un ordinateur de bureau, voir sous la forme d'une carte à mettre dans l'ordinateur. Elles auraient un rôle similaire aux cartes graphiques et ne seraient utilisées que pour de l'accélération.

Idéalement ces unitées devraient offrir la possibilité d'être pilotée soit de façon directe, c'est-à-dire en les mettant directement sur le bus système, soit par l'intermédiaire d'interfaces comme l'USB ou l'éthernet, illustration 5.3. Laisser les deux possibilités de connexion devrait permettre de plus facilement les empiler puis les rendre accessibles sur le réseau. L'idée serait ainsi de disposer d'unités standardisées avec des tailles normalisées, aussi bien au sens dimension qu'au sens nombre de qubits. Empiler des unités de même taille ayant comme intérêt d'améliorer la fiabilité des résultats, et non d'augmenter le nombre de qubit.

Sur l'architecture proposée, illustration 5.3, nous avons possitionné deux processeurs. Le premier, nôté Q-Proc, en celui quantique, tandis que le C-Proc en est un classique. L'idée est d'envoyer à l'unité quantique un algorithme complet, c'est-à-dire un algorithme comportant aussi bien des parties classiques que des passages optimisés quantiques. Chaque partie pouvant tourner sur son processeur respectif, le tout supervisé par un contrôleur. Ce dernier pouvant aussi, idéalement, gérer l'empilement. L'ordinateur faisant la demande se verrait alors déchargé

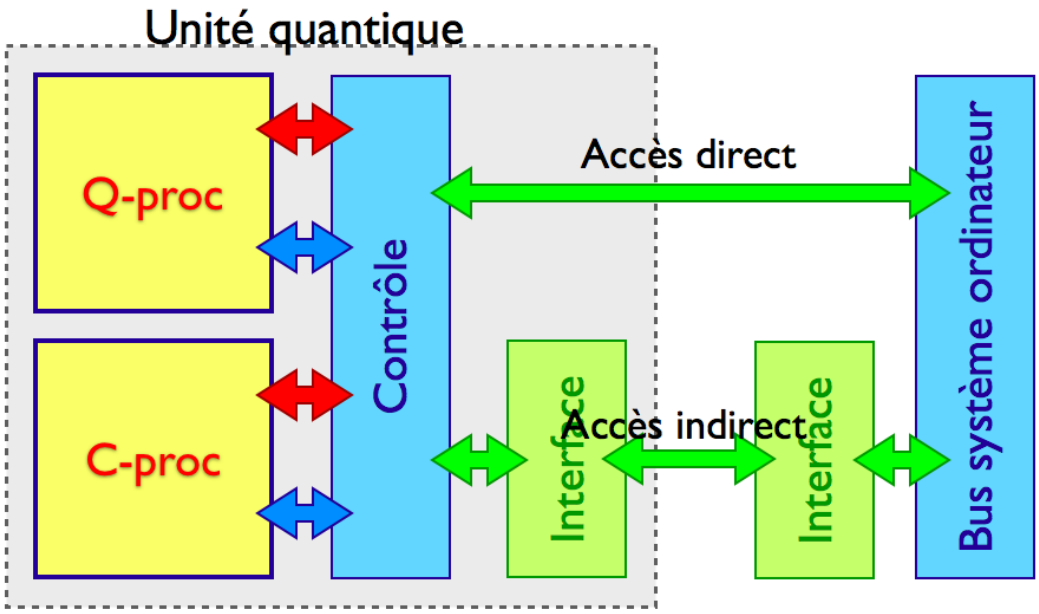

ILLUSTRATION 5.3 – Proposition d'une architecture d'unité quantique.

de toute la complexité et pourrait faire autre chose en attendant l'arrivée du résultat.

Ces propositions permettent de garder le meilleur des deux mondes, classique et quantique, pour arriver à une solution hybride plus facile à réaliser et exploiter. Elles devraient également assurer une transition en douceur vers cette nouvelle informatique.

Chapitre 6

Le processus de changement

Le passage entre un monde où tous les ordinateurs sont “classiques” à un autre où cohabitent ordinateurs “classiques” et quantiques ne se fera pas du jour au lendemain. C’est pourquoi il nous faut réfléchir dès maintenant à comment amorcer cette transition pour qu’elle se fasse le plus en douceur possible.

6.1 Description du processus

6.1.1 Évolution du logiciel

Cette transition ne devra pas se contenter d’être au niveau du *hardware*. Elle devra également comporter une évolution de la partie logicielle. Ceci vient du fait qu’en informatique le logiciel est indispensable pour piloter le matériel.

Nous pouvons retrouver ce besoin, de faire évoluer le logiciel en même temps que le matériel, dans la transition entre processeurs 32 bits et 64 bits. En effet, seuls des logiciels optimisés arrivent à tirer vraiment parti des 64 bits, de la même façon que seuls des algorithmes adaptés peuvent bénéficier de la puissance du calcul quantique.

Cette évolution du logiciel ne consiste pas seulement en une écriture d’algorithmes quantique. Il s’agit d’aller plus loin et d’arriver à offrir la possibilité d’écrire des algorithmes qui puissent à la fois tourner sur des processeurs classiques et être optimisés pour le calcul quantique. De tels logiciels deviendraient alors “universels” et capables de s’adapter à la puissance de calcul disponible sur la machine. Pour cela il nous faut réfléchir à une nouvelle manière de concevoir et réaliser les programmes.

6.1.2 Création d’une nouvelle technologie de programmation

Les méthodes de programmation actuelles ne sont pas prévues pour inclure des algorithmes quantiques. Si nous restons dans l’optique de considérer le calcul quantique comme un accélérateur matériel, il nous faudra alors créer une nouvelle façon de programmer.

Encore une fois nous pouvons nous inspirer du passé pour imaginer le futur. Plus précisément, nous pouvons nous baser sur les travaux réalisés dans le cadre du GPGPU [1]. Celui-ci permet d'utiliser des processeurs graphiques pour réaliser des calculs habituellement demandés à un microprocesseur. Ces travaux ont donné naissances à des frameworks tels que l'OpenCL. Là où ils nous intéressent, c'est qu'ils permettent à un même logiciel de tourner sur différentes machines, avec différentes configurations, tout en utilisant à chaque fois le maximum de ressources disponibles.

Si un tel framework venait à être créé, adapté pour le calcul quantique, il permettrait de gérer les unités de calculs quantiques que nous avons évoqués au préalable. Les programmes n'auraient pas à être écrits spécifiquement selon la taille de l'unité de calculs, ils s'adapteraient automatiquement au nombre de processeurs quantiques disponibles. Nous pourrions même imaginer qu'ils seraient capables d'aller rechercher sur un réseau une unité de calcul disponible.

Mais pour pouvoir être réalisé, ce framework aurait besoin qu'il existe une normalisation au sein du matériel, afin qu'il puisse fonctionner pour chaque type d'unité quantique, quel que soit le fabricant.

6.1.3 Adaptation du matériel

L'adaptation du matériel devrait idéalement être réalisée en deux endroits. Tout d'abord, il devrait exister une adaptation au sein de l'architecture des ordinateurs classiques, afin qu'ils puissent plus facilement se coupler à des unités de calcul quantiques. Ensuite il faudrait que ces unités soient conçues de concert avec le framework proposé précédemment, pour qu'elles puissent être compatibles.

Adaptation de l'architecture des ordinateurs

Dans la pratique, cette adaptation n'est pas réellement nécessaire. Il est plus rapide et plus facile d'adapter la technologie quantique pour s'interfacer sur la classique que de faire l'inverse.

Nous le comprenons mieux si nous prenons pour exemple les disques durs. Ceux-ci peuvent être directement connectés sur la carte mère de l'ordinateur via leur interface IDE ou SATA. Mais ils peuvent également être connectés via une interface intermédiaire, comme l'USB ou le FireWire, dans le cadre des disques dur externes. Ils existent également des disques dur SSD sous la forme de cartes PCI.

Dans ce cas, il ne s'agirait pas nécessairement d'adapter l'ordinateur pour pouvoir accepter une unité de calcul. Il s'agirait plus d'adapter l'unité quantique pour qu'elle puisse s'interfacer avec l'ordinateur. Néanmoins, comme pour les disques durs, limiter les intermédiaires reste préférable.

1. General-Purpose Processing on Graphics Processing Units

Adaptation de l'unité de calcul quantique

Bien que concernant un aspect matériel : l'unité quantique, il s'agit plus en réalité d'une question d'ordre logiciel. L'unité de calcul devra nécessairement disposer d'une interface pour être piloté par un ordinateur classique. Comme nous venons de le voir, cette interface devra idéalement être capable d'utiliser des entrées sorties déjà présentes sur la machine. Mais cette liaison ne devra pas seulement être au niveau physique, elle devra l'être aussi au niveau logique.

Ainsi, l'unité de calcul devra être capable de comprendre les ordres qui lui seront donnés. De plus, pour que le framework proposé marche correctement, l'unité devra aussi connaître et communiquer ses caractéristiques :

- son temps de cohérence, pour connaître la durée maximale d'un calcul,
- le nombre de processeurs quantiques,
- le nombre de qubits dans ces processeurs,
- la fiabilité de ses calculs.

Ce n'est qu'en connaissant tous ces paramètres qu'il sera possible de piloter efficacement un calculateur quantique. D'où l'idée proposée précédemment, voir illustration 5.3, de regrouper au sein de de l'unité de calcul proposée deux processeurs : un quantique et un classique, le tout supervisé par un contrôleur. Ceci permettrait de ne pas nécessiter de prendre en compte les caractéristiques citées ci-dessus dans le framework. Les unités seraient des accélérateurs matériels capables d'exécuter des algorithmes classiques, quantiques et hybrides. Il serait également envisageable de construire des accélérateurs sur le même modèle, utilisable depuis le même framework, mais basés uniquement sur des processeurs traditionnels, ceux-ci seraient alors moins chers à fabriquer. Nous disposerions alors d'une gamme de calculateurs basés sur une unique façon de programmer.

Ceci reste dans l'optique de proposer une transition en douceur. Il est déjà possible de concevoir le framework et de réaliser la version purement classique de ces accélérateurs. Une fois la version hybride quantique / classique disponible, il ne suffira que de changer l'accélérateur.

Chapitre 7

Les apports du travail

La réalisation de ce mémoire m'a surtout apporté au niveau de la gestion du temps. Savoir comment organiser son travail pour essayer de fournir les livrables demandés en temps et en heure. Il m'a fallut "jongler" en même temps avec le projet de synthèse de l'université et la gestion de projet associée. Le tout en ayant peu de temps lors des phases entreprises à cause des horaires de travail et du temps de transport. Tous ces facteurs ont nécessité d'être capable de passer rapidement d'un travail à un autre pour tenter de respecter les délais demandés tout en évitant de se retrouver submerger. Sur ce premier point, la rédaction de ce mémoire m'aura donné beaucoup d'expérience.

Il m'aura permis de travailler mes capacités de recherches et de synthèses. Tout d'abord trouver où est l'information, puis essayer de l'assimiler. Puis tenter d'en extraire les parties les plus importantes pour pouvoir les résumer dans ce mémoire. Tenter d'en tirer les bonnes conclusions et essayer de trouver un moyen de tirer parti d'une technologie qui n'existe pas encore et dont il n'est pas sûr qu'elle sera un jour pleinement fonctionnelle. Tout ceci est un bon exercice cérébral qui pourra me resservir par la suite. Il me sera en effet probablement souvent demandé au cours de ma future carrière de réaliser des études de l'existant afin de trouver la meilleure solution possible à un problème posé.

Finalement, ce mémoire m'aura également permis de renouer avec la physique, qui était mon orientation initiale après le bac.

Chapitre 8

La conclusion et les perspectives d'avenir

Si l'informatique quantique semble en effet prometteuse, elle est loin d'être en mesure d'apporter une révolution. Comme nous l'avons vu les contraintes pour bénéficier du calcul quantique sont trop importantes pour que celui-ci puisse remplacer le calcul classique. Si la faible taille des processeurs pourra vraisemblablement être résolue, il ne semble pas que ce soit le cas pour la décohérence. De même, il ne restera possible que de lire un seul des résultats du parallélisme quantique.

Pour pouvoir pleinement profiter d'un processeur quantique, seules des astuces mathématiques, comme dans le cas de Shor et de Grover, permettent de contourner ces difficultés, mais la décohérence empêche d'avoir de longs algorithmes quantiques. Il ne sera jamais possible de maintenir indéfiniment la cohérence, cela impliquerait une isolation totale des qubits ce qui est techniquement impossible. De plus, ces astuces ne marchent que dans certains cas, ce qui explique pourquoi le nombre d'algorithmes quantiques reste assez restreint.

Néanmoins cette technologie du futur reste prometteuse. Son étude aidera à améliorer les processeurs actuels en permettant de repousser l'apparition de problèmes liés aux phénomènes quantiques. Elle permettra aussi de réaliser des accélérateurs matériels pour certains calculs bien particuliers. Elle pourra également être utilisée pour lancer des simulations de propriétés physiques, mais ceci n'entre pas dans le cadre du calcul quantique à proprement parler.

Les unités de calculs proposées semblent être une utilisation viable de cette nouvelle technologie, connaissant les contraintes associées. Les ordinateurs quantiques ne verront peut-être jamais le jour, dans le sens où les programmes contiendront probablement toujours une grande part de "classique". De plus, les processeurs quantiques risquent de devoir continuer à être contrôlés par des ordinateurs classiques. Néanmoins, l'accélération par le calcul quantique à de meilleures chances de finir par devenir réalité.

Table des illustrations

2.1 À gauche une valeur discrète, à droite une valeur continue 14
2.2 Couleur et classification des étoiles en fonction de leur température de surface . 15
2.3 Représentation d'un électron autour d'un atome : à gauche le modèle quantique, à droite le modèle classique. 17
2.4 Le chat de Schrödinger : mort et vivant à la fois 18
2.5 La sphère de Bloch 19
2.6 Parallélisme quantique : calcul réalisé sur 3 qubits. 20

3.1 Cas favorables et défavorables du problème. 27
3.2 Peter Shor 28
3.3 Vitesse pour la factorisation d'un nombre de 100 bits et moins. 29
3.4 Vitesse pour la factorisation d'un nombre de 100 bits et plus. 30
3.5 Lov Grover 31
3.6 Vitesse de recherche en fonction de la taille d'une base de données. 31

4.1 RMN 34
4.2 Isaac Chuang 34
4.3 Piège pour un ion de strontium. 36
4.4 Le processeur de D-Wave 38
4.5 Jonction Josephson 39

5.1 Le cray 1 est un des plus célèbres superordinateurs. Il est reconnaissable à sa forme en arc de cercle. Il utilise un unique processeur vectoriel 64 bits. 44
5.2 Exemple d'architecture SIMD, le même calcul est effectué sur 4 jeux de données différentes 44
5.3 Proposition d'une architecture d'unité quantique. 48

9.1 Dr Daniel Esteve 57
9.2 Dr Julia Kempe 62

Bibliographie

[Asp] Aspect, Alain. Le débat bohr-einstein et l'intrication quantique à l'épreuve de l'expérience. http://www2.cnrs.fr/sites/communique/fichier/debat.pdf.

[Bud] Budnik, Paul. Measurement in quantum mechanics faq : Schrödinger's cat. http://www.mtnmath.com/faq/meas-qm-3.html.

[Cho11] Cho, Adrian. Controversial computer is at least a little quantum mechanical, 2011. http://news.sciencemag.org/sciencenow/2011/05/controversial-computer-is-at-lea.html.

[CNR11] Quantum computers : The ultimate challenge. *CNRS international magazine*, 2011.

[Col07] Colin Johnson, R. Quantum computer 'orien' debuts, 2007. http://www.eetimes.com/electronics-news/4069654/Quantum-computer-Orion-debuts.

[Div00] Divincenzo, David P. The Physical Implementation of Quantum Computation. *Fortschr. Phys.*, 48(9-11) :771–783, 2000.

[DW] D-Wave. Press releases. http://www.dwavesys.com/en/pressreleases.html.

[Est05] Estève, Daniel. Vers des processeurs quantiques ? *Les clefs du CEA*, 52 :18 – 27, 2005.

[Gan11] Ganier, Aude. Au coeur de la supraconductivité. 159 :6 –10, 2011.

[Gra] Grangier, Philippe. Groupe optique quantique. http://www.cnanoidf.org/Groupe-Optique-Quantique.

[Hag11] Amit Hagar. Quantum computing. In Zalta, Edward N., editor, *The Stanford Encyclopedia of Philosophy*. Spring 2011 edition, 2011.

[Hol73] Holevo, A. S. Some estimates of the information transmitted by quantum communication channels. *Problemy Peredaci Informacii*, 9(3) :3–11, 1973.

[Jon] Jones, Andrew Zimmerman. Schroedinger's cat - what is schroedinger's cat ? http://physics.about.com/od/quantumphysics/f/schroedcat.htm.

[Lac07] Lacour, Xavier. *Information Quantique par passage adiabatique : Portes quantiques et décohérence*. PhD thesis, Université de Bourgogne, 2007. http://tel.archives-ouvertes.fr/docs/00/18/08/90/PDF/These.XL.pdf.

[Mer07] Mermin, N. David. *Quantum Computer Science : An Introduction*. Cambridge University Press, 1 edition, September 2007.

[OLL+02] Orlando, T. P. , Lloyd, S. , Levitov, L. S. , Berggren, K. K. , Feldman, M. J. , Bocko, M. F. , Mooij, J. E. , Harmans, C. J. P. , and Wal, C. H. Van Der. Flux-based superconducting qubits for quantum computation. *Physica C*, 376 :194–200, 2002. http://www.ece.rochester.edu/projects/sde/publications/eucas01/eucas01.pdf.

[Pou08] Poulin, David. Codes correcteurs quantiques, 2008. http://www.physique.usherbrooke.ca/~dpoulin/Documents/Sherbrooke08.pdf.

[QOG] California Institute of Technology Quantum Optics Group, Norman Bridge Laboratory of Physics. Quantum teleportation. http://www.its.caltech.edu/~qoptics/teleport.html.

[Rib05] Ribeiro, Pedro. *A new readout method for the quantronium qubit circuit*. PhD thesis, 2005. http://wslc.math.ist.utl.pt/ftp/pub/RibeiroP/05-R-DEAReport.pdf.

[RP00] Rieffel, Eleanor and Polak, Wolfgang. An Introduction to Quantum Computing for Non-Physicists. *ACM Computing Surveys*, 32(3) :300–335, September 2000.

[SHOM06] Stick, D., Hensinger, W. K., Olmscenk, S., and Monroe, C. Semiconductor traps for laser-cooled atomic ions and scalable quantum computing, 2006. http://www.sussex.ac.uk/physics/iqt/LEOS_june06_article.pdf.

[Vio06] Vion, Denis. En route vers l'ordinateur quantique ?, 2006. http://www.phys.ens.fr/enseign/fip/seminaires/rapports/vion.pdf.

[VYC00] Vandersypen, L. M. K. , Yannoni, C. S., and Chuang, I. L. Liquid state NMR Quantum Computing. *ArXiv Quantum Physics e-prints*, December 2000. http://qt.tn.tudelft.nl/~lieven/papers/ENC_nmr.pdf.

Chapitre 9

Interviews d'experts

9.1 Interview du Docteur Daniel Esteve

Date de l'interview : Lundi 04 avril 2011

Lieu de l'interview : Laboratoires du groupe Quantronique, CEA-Saclay

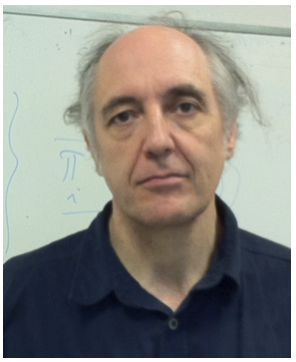

ILLUSTRATION 9.1 – Dr Daniel Esteve

Méthodologie employée :
- prise de notes sur un calepin
- enregistrement de l'interview sur un iPhone

Présentation de l'interviewé :

Le Docteur Daniel Esteve est l'un des trois fondateurs du groupe Quantronique, en 1984. L'objectif de ce laboratoire est la fabrication et l'utilisation de circuits électroniques se comportant suivant la mécanique quantique. Le groupe Quantronique fait actuellement parti du Service de Physique de l'État Condensé, au sein de l'Institut Rayonnement Matière de Saclay (centre de recherche du CEA, Commissariat à l'Énergie Atomique et aux Énergies Alternatives).

Suite à ses travaux, le Docteur Daniel Esteve a obtenu le prix Agilent Europhysics en 2004.

Informations de contact :
- téléphone : ***+33 1 69 08 66 29*** (numéro du groupe Quantronique)
- courriel : ***daniel.esteve@cea.fr***

9.2 Contenu de l'interview

Pouvez-vous décrire les objectifs du groupe quantronique ?

Les objectifs du groupe Quantronique sont de réaliser des circuits électriques qui se comportent de façon véritablement quantique au sens où les variables d'état électriques comme les tensions et les courants sont des variables quantiques. La mécanique quantique ne régit pas seulement l'évolution des électrons individuels, mais aussi celle du circuit complet. Cela peut aller à placer le circuit dans une superposition d'états correspondants à des courants circulant dans des directions opposées dans le même fil ! Ce sont ces superpositions qui donnent accès à la puissance de la mécanique quantique pour le calcul. Mais là, Quantronique ne s'intéresse pas uniquement à l'information quantique, mais aussi aux phénomènes quantiques dans les circuits électriques en général.

Pour résumer, il s'agit de développer une électronique véritablement quantique, où la mécanique quantique est nécessaire pour décrire l'état du circuit complet.

Dans la littérature on retrouve souvent la notation $|\psi\rangle$ comment l'appelez-vous ?

C'est la notation de Dirac pour un état quantique avec la lettre grecque psi, entre un bra et un ket (bracket signifie crochet en anglais).

Dans quel état mettez-vous le circuit lors de sa préparation ?

Nos circuits à bits quantiques se mettent spontanément dans leur état de plus basse énergie, noté 0, à basse température.

À partir de cet état, nous pouvons préparer toute superposition $|\alpha 0 + \beta 1\rangle$ des états 0 et 1 du bit quantique avec des coefficients complexes arbitraires α et β. La lecture du qubit après cette préparation donne les valeurs 0 et 1 avec des probabilités proportionnelles au module au carré des coefficients de la superposition.

La préparation de ces états superposés suivis de leur lecture est l'expérience dite des oscillations de Rabi. Isaac Rabi est un physicien américain qui a été le premier à réaliser des oscillations cohérentes avec des atomes. C'est une expérience fondatrice de la mécanique quantique.

Dans un article parlant du quantronium il était fait mention de la durée de vie du circuit, pourriez-vous en parler ?

Tout d'abord, le quantronium est un circuit qui est dépassé et que nous n'utilisons plus.

Quand on parle de la durée de vie, on parle en fait de deux durées de vie.

Quand on prépare l'état 1, il y a la durée de vie T1 correspondant au temps de relaxation vers l'état 0. Il s'agit du temps au bout duquel le système sera retombé à l'état 0. Quand on prépare un état $|\alpha 0 + \beta 1\rangle$ il y a le temps T2, le temps de cohérence. C'est la durée pendant laquelle l'information de phase est gardée, pendant laquelle on peut dire que ce système est réellement avec les coefficients de départ.

Actuellement, dans les circuits nanofabriqués, T1 et T2 sont de l'ordre de la microseconde. Très récemment, un gain d'un facteur 10 a été réalisé à Yale mais au prix de certaines limitations assez gênantes, à notre avis.

Ce qui compte réellement est le nombre d'opérations que l'on peut réaliser pendant le temps T2, il est possible actuellement d'en réaliser quelques dizaines.

Au groupe Quantronique, combien de qubits arrivez-vous à utiliser en même temps ?

Nous avons un processeur opérationnel avec deux qubits, muni d'une lecture indépendante en un coup de chaque qubit, et de portes quantiques capables de réaliser toutes les évolutions quantiques possibles avec ces deux qubits. Nous avons très récemment démontré l'algorithme de recherche de Grover d'un objet parmi quatre en un seul pas d'algorithme.

Quel est l'état de l'art ?

L'équipe de Yale a mis en œuvre un processeur à trois qubits, mais sans lecture en un coup et donc sans véritable gain quantique pour les algorithmes démontrés expérimentalement.

L'équipe de John Martinis à l'université de Santa Barbara (UCSB) dispose d'un système avec quatre qubits et lecture en un coup, mais n'a pas encore mis en oeuvre d'algorithme quantique.

Il y a aussi TUDelft qui a fait un processeur à 2 qubits, mais qui n'est pas encore fonctionnel.

Pour la cohérence, c'est Yale qui est le plus avancé avec des qubits dans des cavités micro-ondes 3D. Pour la lecture ce serait plutôt le CEA. En ce qui concerne processeur + lecture, ce serait plutôt en faveur de l'UCBS.

Les équipes que vous venez de citer ne concernent bien uniquement les processeurs à base électronique ?

Oui, si nous ne considérons que les circuits supraconducteurs, ce que les équipes que je viens de citer définissent l'état de l'art. Mais en information quantique il y a aussi les ions piégés avec

plusieurs équipes très avancées.

Pensez-vous qu'il existera un jour un ordinateur purement quantique ?

Les qubits ne sont intéressants que pour des phases où le calcul peut bénéficier du gain exponentiel de certains algorithmes quantiques.

Avec la miniaturisation des composants, les processeurs se rapprochent de la frontière en physique classique et physique quantique. Pensez-vous que vos recherches auront un impact pour la réalisation des processeurs classiques ?

Le problème de la physique quantique dans les processeurs classiques se trouve au niveau des composants. À ce niveau-là il existe en effet des problèmes de physique quantique qui apparaissent dans les processeurs classiques. Cela peut créer un véritable mur pour la miniaturisation. Ainsi, les CMOS devenant de plus en plus petits, des effets quantiques apparaissent dans la physique de l'effet de champ. Mais ces problèmes n'ont rien à voir avec le calcul quantique. Il s'agit là de mécanique quantique au niveau du composant alors que pour le calcul quantique il faut la mécanique quantique au niveau du circuit complet.

En définitive un ordinateur quantique ne pourra jamais remplacer un ordinateur quantique ? Ils seront plutôt complémentaires ?

L'ordinateur quantique n'a de l'intérêt que s'il y a un algorithme qui va plus vite que celui qui tourne sur une machine classique, or il n'existe pas beaucoup d'algorithmes quantiques aujourd'hui.

À part Grover et Shor, existe-t-il d'autres algorithmes ?

Il existe quelques autres algorithmes quantiques, Mais l'algorithme de Shor permet de résoudre d'autres problèmes dans la même classe de complexité, comme le problème d'optimisation du voyageur de commerce. On pense en effet que si on est capable de résoudre un problème complexe donné, alors on est capable de résoudre tous les problèmes de la même classe de complexité. En définitive, même s'il y a peu d'algorithmes quantiques, ils peuvent servir à beaucoup de choses.

La voie la plus prometteuse semble toutefois la simulation de systèmes quantiques car elle est très difficile à effectuer avec un ordinateur classique.

Si un algorithme quantique peut améliorer le problème du voyageur de commerce, est ce parce que grâce au parallélisme quantique toutes les possibilités pour le voyageur sont

testées en même temps ?

Oui, les algorithmes quantiques sont toujours basés sur l'exploitation intelligente du parallélisme quantique. Mais ce parallélisme ne donne pas nécessairement une puissance de calcul particulière.

En effet, même si l'on fait tourner une simulation avec toutes les valeurs possibles des entrées en un coup, la réponse à la sortie est la superposition de tous les résultats possibles. Mais lors de la lecture on ne peut accéder en général qu'à un seul des résultats. C'est pour cela que le parallélisme quantique n'est pas aisément exploitable. Il faut beaucoup d'astuce pour exploiter le parallélisme quantique de façon efficace. C'est toute la beauté de l'algorithme de Shor.

J'ai lu que l'algorithme de Shor à besoin de tourner sur plus de 90 qubits pour devenir plus efficace qu'un algorithme classique.

Je ne suis pas sûr, cela dépend de la taille des nombres que l'on cherche à factoriser.

Le problème des qubits est qu'il faut qu'ils soient munis de leur système de correction d'erreurs.

Il faut donc compter les qubits avec un circuit de correction d'erreur quantique, ce qui augmente leur nombre.

Une dernière question : quel est selon vous le plus gros obstacle actuel ? Est-ce le nombre de qubits que l'on arrive à utiliser dans un circuit, où est-ce le problème de la décohérence ?

Il s'agit du problème de la décohérence. Il existe les fameux critères de Di Vincenzo à satisfaire pour avoir un bon processeur quantique :

- les qubits doivent être intégrables et réalisables en grand nombre,
- il faut disposer de portes quantiques universelles, capables de réaliser tout algorithme.
- il est nécessaire d'avoir une lecture fidèle en un coup.
- il faut pouvoir réinitialiser efficacement chaque qubit dans l'état 0.

Il faut également pouvoir mettre en oeuvre la correction d'erreur quantique. Bien que des algorithmes existent pour cela, ils n'ont pas encore pu être mis en oeuvre car le niveau de cohérence quantique à atteindre pour pouvoir en bénéficier est déjà bien supérieur à celui atteint, pour tous les systèmes à bits quantiques existants aujourd'hui.

9.3 Interview du Docteur Julia Kempe

Date de l'interview : Mardi 19 avril 2011

Lieu de l'interview : Entretien téléphonique

ILLUSTRATION 9.2 – Dr Julia Kempe

Méthodologie employée :
- prise de notes sur un calepin
- appel via le logiciel Skype, pour pouvoir enregistrer l'entretien sur ordinateur

Présentation de l'interviewée

Le Docteur Julia Kempe est actuellement membre du LIAFA, Laboratoire d'Informatique Algorithmique Fondements et Applications, de l'Université Paris VII. Cette femme, passionnée par le calcul quantique, a mené deux thèses en parallèles : une en mathématique et l'autre en informatique. Elle à été cité en Janvier 2011 dans le magazine international du CNRS, dans le cadre d'un article parlant de l'informatique quantique.

Elle a également reçu la distinction Femme en Or de la recherche 2010.

Informations de contact :
- téléphone : ***+33 1 69 08 66 29*** (numéro du groupe Quantronique)
- courriel : ***daniel.esteve@cea.fr***

9.4 Contenu de l'interview

J'ai cru comprendre que votre travail au LRI concerne la partie algorithmique du calcul quantique ?

Oui

Pourriez-vous expliquer comment un algorithme quantique peut être plus rapide qu'un algorithme traditionnel ?

Un ordinateur classique est basé sur le principe de 0 ou 1, tandis que dans un ordinateur quantique on fait en sorte d'avoir 0 et 1 en même temps. Pour y arriver on utilise les principes de la mécanique quantique. Celle-ci décrit les lois de la physique à la plus petite échelle : au niveau des atomes, électrons, etc.

À cette échelle les lois changent, elles diffèrent de ce dont on a l'habitude. Les particules sont décrites par ce que l'on appelle une fonction d'ondes. Cette fonction d'ondes à la propriété de ne pas pouvoir vraiment déterminer la position ou l'état d'une particule. Nous pouvons ainsi décrire un état comme étant quelque chose étant un peu un 0 et un peu un 1.

Nous essayons d'utiliser ce principe pour construire un nouvel ordinateur qui fait mieux que les ordinateurs classiques. Le plus fameux algorithme que l'on connaisse, basé sur ce principe, est l'algorithme de Shor pour la factorisation rapide des nombres. Mais il en existe d'autres.

Sur quoi vous concentrez-vous au LRI ?

En réalité je ne suis plus au LRI, mais au LIAFA, même si ce n'est pas très important.

Je travaille sur plusieurs choses :

- la complexité, c'est-à-dire comprendre quels problèmes seraient faciles ou difficiles pour un ordinateur quantique
- je travaille également sur les problèmes qui exemplifient un peu la difficulté du calcul quantique : des problèmes provenant souvent des systèmes physiques. Ils décrivent une situation physique et je travaille sur les liens entre ces problèmes, provenant de la physique, et leur complexité si on les traite comme problèmes relevant du calcul quantique. Le problème des hamiltioniens, matrices permettant de déduire les propriétés des systèmes : leur énergie, etc. est l'un des problèmes utilisés pour classifier la difficulté des problèmes en calcul quantique.

L'algorithme de Shor pour la factorisation des nombres, celui de Grover pour la recherche des données… les algorithmes quantiques peuvent-ils être utilisés pour tous les types de calculs que l'on attend dans un ordinateur traditionnel ?

Déjà, nos ordinateurs traditionnels ne sont pas si mauvais que ça. Pour les petits calculs que vous faites, où l'ordinateur classique est bien adapté, il n'y a pas besoin d'utiliser un ordinateur quantique. Ensuite l'ordinateur quantique n'existe pas encore, sa construction est un défi formidable. Personnellement je n'en utiliserais pas un pour des choses qu'un ordinateur classique sait déjà bien faire. Je l'emploierais plutôt pour des choses difficiles, comme la factorisation, la simulation des systèmes quantiques, ou pour connaître certaines propriétés des systèmes, etc.

Si un ordinateur quantique n'est pas des plus efficaces pour les problèmes traditionnels, quels sont les problèmes pour lesquels ils sont les plus amène à être utilisés ?

Je n'ai pas dit qu'ils n'étaient pas efficaces. Si on arrivait à en construire un il serait tout aussi efficace qu'un ordinateur classique. Il pourrait faire tout ce que peut faire un ordinateur classique, mais le problème est de le construire. Il faut avoir une quantité de qubits : des bits quantiques.

Laissez-moi reformuler ma question. Il existe des algorithmes, comme Shor, où le quantique est beaucoup plus rapide que le classique. Pour quels domaines de calculs le quantique serait beaucoup plus efficace que le classique ?

C'est une bonne question, elle fait le sujet de recherches par beaucoup de personnes.

Actuellement nous avons quelques problèmes où un ordinateur quantique est « beaucoup mieux » qu'un ordinateur classique : l'algorithme de factorisation de Shor, un algorithme d'inversion de logarithmes, ainsi que le problème des sous-groupes cachés. Il s'agit d'un cadre général pour tous ces problèmes où un ordinateur quantique est bien meilleur qu'un ordinateur classique.

Par contre il existe des problèmes où un ordinateur quantique est meilleur qu'un ordinateur classique, mais sans être extrêmement meilleurs. Il existe tout un groupe d'algorithmes dans ce cas-là. Le premier est l'algorithme de Grover pour la recherche, où un ordinateur quantique est quadratiquement plus rapide qu'un ordinateur classique. C'est-à-dire que si un ordinateur classique à besoin d'un temps t, l'ordinateur classique n'a besoin que d'un temps racine de t. Il y a ainsi plusieurs problèmes liés à la recherche de choses.

J'ai lu que vous aviez exploré à la fois la partie mathématique et la partie informatique du calcul quantique, mais que vous aviez également étudié avant la partie physique. Pourriez-vous en parler ?

Je l'ai étudié un peu avant oui, il y a maintenant quelques années. Comme je l'ai dit, le grand défit est de construire un ordinateur quantique. Actuellement si on n'y arrive pas, c'est à cause du bruit, que l'on appelle décohérence, qui fait que les qubits, cette magnifique superposition de 0 et de 1 va être « cassée ». Nous ne pouvons donc pas utiliser le fait que cette particule est dans l'état 0 ET 1. Or nous en avons besoin pour réaliser des calculs de meilleure façon que dans

le domaine classique. Le grand défit lors de la construction est de trouver une parade contre la décohérence. C'est sur cela que j'ai travaillé. Je cherchais quels types de codages, quels types de systèmes peuvent être construits qui ne souffrent pas tellement de la décohérence. J'ai étudié les bruits physiques pour voir ce qui pouvait être fait.

Même si ce n'est pas tout à fait dans votre domaine, parmi les trois voies de recherches suivantes : les ions piégés, la résonance magnétique nucléaire et les circuits supraconducteurs, laquelle vous semble la plus prometteuse ?

C'est difficile à dire, mais d'après ce que je comprends, la résonance magnétique nucléaire ne se fait pas très bien à grande échelle, même s'il est vrai qu'on l'a utilisé pour le premier algorithme vraiment implémenter : Shor. Mais il est difficile de voir comment faire quelque chose de plus grand. On utilise une molécule et on « parle » à ses élections avec des lasers, mais il devient de plus en plus difficile de « parler » à de plus en plus d'électrons. Or c'est ce qu'il devrait être fait si l'on voulait avoir plusieurs, voir beaucoup, de qubits.

Les circuits supraconducteurs c'est quelque chose qui est essayé, mais je ne peux pas très bien en parler parce que je ne sais pas quels sont les problèmes rencontrés avec les circuits.

En ce qui concerne les ions piégés, je ne sais pas trop, parce qu'il faut aussi piéger les ions, et je ne pense pas que l'on puisse en piéger trop.

Si je devais en choisir un, ça serait le troisième, les supraconducteurs, mais je ne peux pas en dire grand-chose. Mais la résonance magnétique nucléaire ne marchera pas à grande échelle. Je ne pense pas que si on veut avoir 100 qubits, voir 1 000 qubits cela puisse aller.

Pensez-vous que les recherches en informatique quantique vont avoir un impact sur la construction des processeurs classiques ? Ou les deux continueront-ils à être développés indépendamment ?

Pour le moment cela serait plutôt de façon indépendante. Mais il faut savoir que les microprocesseurs deviennent actuellement de plus en plus petits. Vous connaissez sans doute la loi de Moore qui dit que tous les 18 mois la taille de nos microprocesseurs devient deux fois plus petite pour le même pouvoir. À un certain moment, l'échelle quantique sera atteinte. Il se produira alors des effets quantiques, que l'on le veuille ou non.

Je pense que dans ce sens il est déjà intéressant d'étudier maintenant les effets quantiques, ce qu'ils peuvent donner, parce que de toute façon d'ici quelques années nous seront dans ce régime. Même s'il est vrai qu'en général on nous demande maintenant qu'est-ce qui peut être fait pour éviter les effets quantiques qui "pourrissent" les microprocesseurs. Pour cette question il est possible de donner quelques réponses. Mais pour nous la question est inverse : qu'est-ce que l'on peut faire pour utiliser les effets quantiques ?

Pensez-vous voir arriver deux informatiques, une avec des microprocesseurs classiques qui s'arrêtent à la frontière entre classique et quantique, et une autre avec des processeurs quantiques ?

Je ne sais pas si cela sera comme cela, mais je pense que de toute façon les gens ne pourront bientôt plus ignorer la mécanique quantique à un certain niveau. Ils ne feront peut-être pas un petit ordinateur quantique, mais ils s'appuieront sur ce que nous faisons, même si c'est nos travaux sur la décohérence, etc. Ils verront comment procéder pour avoir de meilleurs microprocesseurs, mais je ne peux pas vraiment prédire comment ils seront.

Même si l'on était capable de construire un ordinateur quantique, serait-on capable de vraiment l'exploiter ? Avec le nombre encore restreint d'algorithmes et la difficulté à mettre beaucoup de qubits, serait-il vraiment utilisable ?

C'est une bonne question, plusieurs personnes travaillent dessus.

Il existe tout un autre domaine qui est la simulation des propriétés de la matière. Nous voulons décrire une matière qui possède des effets quantiques et nous voulons connaître une propriété, comme l'énergie. Cela est difficile à faire avec un ordinateur classique parce que cela devient trop grand. Les matrices à utiliser sont trop grandes pour pouvoir le faire de manière efficace, cela prend donc beaucoup de temps. Dans ce cas-là, je pense qu'un ordinateur quantique, même à 200, 300 qubits, peut être vraiment efficace.

Il existe aussi le domaine de la crypto quantique, qui comme vous le savez sans doute déjà, utilise de plus petits systèmes de qubits, basés sur des photons, pour la crypto-distribution des clefs, etc. Mais je pense que les cryptographes quantiques, avec un petit système, disons 100 qubits, pourraient faire beaucoup de choses en crypto-quantique que l'on ne peut pas faire classiquement. Je ne suis pas trop experte en ce domaine, mais je pense qu'ils seront très contents d'avoir un ordinateur quantique, même petit.

Pour casser des clefs de cryptage ?

Non, plutôt pour des choses constructives, comme la distribution de clefs. Mais il existe d'autres protocoles, comme l'authentification quantique, qui sont basés sur des états avec un nombre limité de qubits, peut être une centaine, mais pas plus. Ce genre de choses peut être fait avec de petits ordinateurs quantiques : de la crypto fiable.

Que pensez-vous être le plus grand progrès en informatique quantique depuis l'algorithme de Shor ?

C'est une très bonne question, mais qui reste subjective. Personnellement je trouve que l'on a une meilleure compréhension de ce qui peut et ne peut pas être fait pas un ordinateur quantique. Il y a eu beaucoup de progrès dans le domaine de la complexité quantique, pour classifier les

problèmes en facile, difficile, pour un ordinateur quantique. Je n'ai pas de résultat en tête qui soit comme Shor mais après Shor. Je ne pense pas qu'il y en a eu, mais il existe de nombreux progrès qui petit à petit avancent le domaine.

Il existe aussi des résultats intéressants qui utilisent les outils quantiques pour commencer à prouver ou à comprendre des choses provenant du domaine classique. En théorie de complexité on utilise une technique qui provient de l'information quantique pour prouver quelque chose que l'on ne pourrait pas prouver autrement. Je trouve cela assez fascinant.

Une dernière question : n'est-il pas difficile de travailler sur les algorithmes quantiques alors que vous n'avez pas d'ordinateur quantique à porté de main pour les tester ?

Cela est un peu difficile, mais non pas parce que nous ne pouvons pas faire de tests.

De toute façon, nous faisons de la théorie, nous prouvons des choses de façon très rigoureuse. Je n'ai pas besoin d'un ordinateur quantique pour tester quoi que ce soit. Mais ce qui est frustrant c'est de faire des algorithmes pour une machine qui n'existe pas.

Nous pouvons comparer cela à Babbage qui au XIXe siècle à donné les bases de ce qu'est un algorithme. Mais il n'existait pas d'ordinateur à l'époque, il a fallut attendre 100 ans avant que cela ne devienne applicable. Il n'en reste pas moins qu'il s'agissait de travaux très intéressant et innovateurs. Nous sommes un peu dans la même situation.