Chapter 1

Introduction

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

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

Néanmoins, les composants des systèmes électroniques et optiques de traitement de l'information s'approchent des tailles nanométriques et les limites de validité de la physique classique sont atteintes. Le traitement de l'information stockée aux échelles de distances et de temps atomiques ou moléculaires doit tenir compte des lois de la physique quantique valable à ces échelles. En effet le caractère universel et purement mathématique de la théorie de l'information classique n'est plus valable à ces échelles et doit être repensé pour tenir compte des lois naturelles quantiques. En fait des changements conceptuels radicaux par rapport aux concepts classiques sont nécessaires. La notion de bit classique, $x \in \{0, 1\}$, qui est l'unité de base de l'information classique, doit être complètement révisée. Nous introduirons la notion de "bit quantique" - le qubit - qui possède un caractère "à la fois dis-

cret et continu". Très curieusement, nous verrons qu'un bit quantique est un vecteur à deux composantes complexes continues, mais qui répond de facon discrète quand il s'agit d'en extraire de l'information! Le qubit est l'unité de base de l'information quantique. Les notions d'observation, de mesure et de stabilité d'un état du qubit doivent également être révisées en profondeur.

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

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

Le **chapitre 2** est une description semi-historique des expériences de base (les expériences d'interférences et l'effet photoélectrique) mettant en évidence la dualité onde-particule. Cette nature duale de la matière est à la base de la notion d'état quantique et forme aussi la base de la notion de bit quantique - le qubit - lequel posède une nature duale continue/discrète. Le qubit généralise la notion de bit classique et forme l'unité de base de la théorie de l'information et du calcul quantique.

La nature abonde de degrés de libertés qui sont exactement ou approxi-

mativement représentés par des qubits. Ainsi les qubits sont une ressource naturelle! Deux exemples fondamentaux de qubits exacts sont introduits dans le **chapitre 3**: la polarisation des photons et le spin 1/2 des électrons. Certains des principes de la physique quantique sont illustrés sur ces exemples.

Le **chapitre 4** introduit de facon plus formelle les lois quantiques et les éléments du formalisme mathématique que nous utiliserons. En théorie de l'information et calcul quantique nous avons principalement besoin du formalisme quantique pour des degrés de liberté discrets et nous nous limitons donc à ce cadre, ce qui est en fait une grande simplification. La mécanique quantique des degrés de libertés continus ne sera pas abordée dans ce cours, bien que le sujet soit bien sûr très important. La situation est analogue au cas classique où le traitement digital de l'information ne requiert pas ou très peu de la théorie du traitement des signaux continus.

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

Les **chapitres 5 et 6** introduisent les protocoles à la base de la théorie des communications quantiques. Tout d'abord nous exposons au chapitre 5 le célèbre protocole de Bennett et Brassard (1984) qui permet la distribution d'une clé secrète entre deux acteurs distants Alice et Bob. L'étude de ce protocole est une bonne illustration du "postulat de la mesure" (introduit au chapitres 3 et 4) de la physique quantique.

Le chapitre 6 aborde les protocoles de "codage superdense" et de "téléportation". Ces protocoles très importants mettent en évidence une ressource nouvelle présente en information quantique et qui n'a pas de contrepartie classique. Cette ressource provient de la possibilité "d'intriquer" deux systèmes (les qubits d'Alice et Bob par exemple). Comme nous le verrons l'intrication est une forme de corrélation qui n'a pas d'analogue classique: en particulier ce type de corrélation quantique - appelée intrication - ne peut pas être décrit par des variables aléatoires classiques. Nous verrons comment cela suit des inégalités de J. Bell (1964) et des expériences d'Aspect-Grangier-Roger (1981).

Le calcul et les algorithmes quantiques sont introduits aux **chapitres 7 et 8**. Dans le chapitre 7 nous introduisons un modèle de calcul populaire dû à D. Deutsch (1985) - le modèle des circuits quantiques - qui est en fait une généralisation du modèle classique des circuits. Les circuits quantiques sont constitués de "portes logiques quantiques" universelles généralisant les portes classiques AND, OR, XOR, TOFFOLI et permettant de simuler une large classe de "calculs". Dans cette optique un algorithme quantique est un circuit initialisé dans un état approprié de plusieurs qubits et produisant un état de sortie. Le processus de mesure (d'observation) sur l'état sortant

des qubits produit le résultat du calcul. Comme nous le verrons ce processus de mesure donne un résultat aléatoire, et de ce point de vue les algorithmes quantiques sont des algorithmes aléatoires. Néanmoins le circuit quantique lui-même est déterministe.

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

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

Le **chapitre 9** aborde la dynamique du spin 1/2 dans des champs magnétiques. Cela nous permettra de décrire l'implémentation des portes logiques à un qubit telles que NOT et Hadamard (cette dernière n'a pas d'analogue dans les circuits classiques).

Le **chapitre 10** aborde la question des portes à deux qubits telles que

XOR ou Control-NOT. Cette implémentation est beaucoup moins facile dans la mesure où il faut controller l'intéraction entre deux qubits. Heureusement, comme nous le verrons, la nature nous offre des intéractions appropriées entre moments magnétiques (intéractions de Heisenberg).

Le **chapitre 11** conclu le cours par un survol de la réalisation de circuits et d'algorithmes quantiques. Nous discutons brièvement des expériences implémentant avec succès l'algorithme de Shor pour une dizaine de qubits (~ 2000).

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