Catherine Eng
Martin Prieur de la Comble
Abel Derderian

Avril 2014
Efrei 2013-2014, PL1

TAI d'Atome à la puce : Le processeur quantique

Partie 1 : Introduction générale

On parle d'ordinateur quantique ou de supercalculateur pour les machines disposant de processeur quantique. Cette technologie repose sur la propriétés physique des bits du processeur, qui d'ailleurs ne sont pas des bits mais des « **qubits** » (quantuum – bits).

Par définition, un bit possède deux valeurs : 1 ou 0. Cependant, via la physique quantique, les qubits peuvent avoir ces deux valeurs simultanéement : 0 ET 1. Par conséquent, le traitement des informations est grandement multiplié, et donc les puissances de calcul également.

Le principe est de générer des conditons « parfaites » pour le supercalculateur, à savoir le plonger dans un caisson pour reproduire un environnement qui limite au maximum les interactions avec le monde :

- La pression dans le caisson est environ **10 000** fois inférieure à la pression atmosphérique.
- On met le calculateur dans des températures extrêmement basses. en milieu cryogénique.
- On essaie de rendre nul les champs électromagnétique pour ne pas influer les qubits

Par conséquent, dans l'idée de mettre le moins possibles d'interférences avec le calcul, le traitement d'informations ne se fait pas en temps réel mais en différé : On introduit les données à calculer, le supercalculateur traite les données et seulement ensuite on sort les résultats pour les interpréter.

Nous essaierons donc de présenter l'ordinateur quantique, son interêt, les enjeux qu'il constitut et nous finirons pas conclure en parlant de l'avancée actuelle de ce domaine, et des applications qu'il pourrait avoir dans le futur.

L'intérieur d'un calculateur quantique.

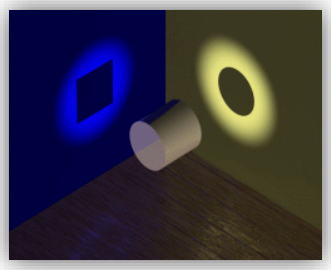
Le processeur quantique se situt à l'extrémité du calculateur, en bas.

Partie 2 : Présentation physique

2.1) L'ordinateur quantique

Découvert en 1985 par le Britannique physicien David Deutsch, un ordinateur quantique est une machine qui fonctionne en accord avec le principe des mécanismes quantiques, la physique de petits éléments tels que les électrons et les photons.

Avec un ordinateur classique, le transistor range chaque bit de l'information. Si le transistor est fonctionnel, c'est un 1. S'il ne fonctionne pas c'est un 0.



Avec l'ordinateur quantique, l'information est reportée dans un système qui existe en deux parties qui fonctionnent en même temps, c'est ce que l'on appelle la **superposition** des principes de la mécanique quantique.

← *L'illustration concrète de la dualité de l'état quantique*

Le **qubit** est la contraction de quantum Bit (bit quantique), c'est une évolution du bit, puisque à l'instar du bit normal (qui est boléen, à savoir qu'il n'a que deux valeurs possibles, **0** et **1**), le qubit est dans un état constant de superposition. En effet, grâce à l'émulation d'un environnement extrrémement spécial, on sait utiliser les propriétés quantiques de la matière : le qubit est constamment excité et peux donc prendre ses deux valeurs simultanément

01000001

Ce « **qubit** » peut stocker un 0 et un 1 en même temps. Si on construit 2 qubits ils peuvent contenir 4 valeurs à chaque fois par exemple 00, 01, 10 et 11. Au fur et à mesure que l'on rajoute des « **qubits** » on peut générer une machine exponentiellement plus puissante qu'un ordinateur classique.

2.2) L'environnement du supercalculateur

Pour travailler avec les propriétés quantiques des matériaux dans les supercalculateurs, on doit simuler un environnement bien particulier. En effet, il est pour l'instant quasiment impossible (ou du moins très compliqué) d'utiliser un ordinateur quantique en directe : la méthode actuelle consiste a insérer les données préalablement dans le calculateur, le plonger dans un caisson, lancer le calcul des données et finalement on sort l'ordinateur quantique de son caisson pour en extraire et analyser les données.

Ce caisson dispose de plusieurs caractéristique :

- Il maintient une température extrême dans le caisson.

Afin de générer le phénomène de **supraconductivité**, on refroidit le calculateur à une température extrême de **30mk**, donc presque au zéro absolu (qui est d'environ **-273,15 °C** ou 0 K) via de l'**azote liquide**, ce qui permet d'obtenir une absence de résistance électrique (donc arrêt des pertes d'énergies) dans le déplacement des électrons.

- Il essaie d'isoler le calculateur de tout champ électromagnétique.

Le calcul des ordinateurs quantiques se fait donc avec le qubit, qui tire son interêt de son excitation électrique. Afin de ne pas troubler le calcul, on doit essayer isoler l'ordinateur (lorsqu'il est plongé dans son caisson) de tout champ électromagnétique pour ne pas que cela influe sur les calculs.

Partie 3 : Enjeux

3.1) Avantages et interêts

L'interêt que porte la science pour les calculateurs quantiques est évidente. Depuis la découverte de l'informatique, les chercheurs n'ont cessés de réduire les composants pour améliorer les performances afin de gagner en vitesse, rendements, puissances puisque tout ses facteurs coûtent et peuvent rapporter des économies à de grandes firmes.

La puissance, évidemment, est le facteur premier et c'est même par ça qu'on caractérictise un ordinateur quantique, car on estime qu'un calculateur quantisque serait plusieurs millions de fois plus puissant qu'un ordinateur normal (et donc également plusieurs milions de fois plus rapide). Voyons une liste des plusieurs intérêts qu'un calculateur quantique peut avoir pour la NASA (principal organisme à s'investir dans la matière) et/où la science :

1. La résolution d'algorithme soit extrêmement complexe, soit extrêmement long

Certaines équations ou algorithme mathématique utilisent des composantes dont le comportement croit en exponentiellement extrêmement rapidement, et sont donc quasiment impossible à étudier correctement. C'est notemment le cas de l'équation P = NP, en mathématique (information théorique), qui est considéré comme un des problèmes scientifiques du millénaire. Si des super calculateurs parviennent à résoudre ce problème complexe, on estime que les domaines de la cryptographie, des mathématique, de l'économie, de l'informatique et de l'ingénieurie pourraient connaître une avancée considérable.

2. Le déchiffrage de la cryptographie

C'est un sujet qui rend perplexe de nombreux spécialistes de la cryptographie : les méthodes de cryptage informatique actuelle, tel que le SHA256 (une des plus puissantes actuellement) sont étudiées et générées pour qu'il soit calculatoirement impossible de trouver la signification du message crypté. Cependant, en améliorant la puissance et la vitesse de calcul tel que le ferait un supercalculateur quantique par rapport à un supercalculateur actuel, il deviendrait alors sans doute possible de « casser » les clefs de cryptage.

3. Réduction des couts

En effet, si un ordinateur quantique permet d'effectuer le travail de plusieurs dizaines, voir centaine, de super-calculateurs, sachant que ceux-ci sont extrêmement consommateur et tournent longtemps à l'heure actuel : des économies non-négligeables en tant de calcul, de consommation mais aussi de place pourront être effectuées par les firmes diposant de ses ordinateurs.

Partie 4 : Historique

4.1) Naissance du calculateur quantique

La naissance de l'ordinateur quantique date des années **1980**, lorsque le physicien Richard Feynman évoque l'idée d'utiliser la physique quantique dans nos calculateurs. Pendant longtemps on douta quant à la possibilité d'exploiter cette idée… Jusqu'au jour où, en 1994, le chercheur **Peter Shor** parvient à prouver qu'il est possible d'utiliser la physique quantique pour la factorisation de grand nombre dans un temps record. Cette découverte leva alors tous les doutes sur la physique quantique et son utilisation et de nombreux projets virent alors le jour.

4.2) Les premiers ordinateurs quantiques

En 1998, IBM est la première société à présenter un calculateur quantique de **2 qubits**. Les années suivantes, IBM utilisera **l'algorithme de Grover**, créé en 1996 par le chercheur Lov Grover, ainsi que **l'algorithme de Shor**, créé en 1994 par Peter Shor. Ce dernier algorithme permet la factorisation de grands nombres en un temps raisonnable, ceci grâce à la physique quantique. En décembre 2001, IBM parvient, grâce à cet algorithme, à factoriser le nombre 15 avec un calculateur quantique de 7 qubits.

4.3) La société D-Wave

En février 2007, la société D-Wave assure avoir mis au point un calculateur quantique stable de **16 qubits**. Ces machines fonctionneraient grâce à une puce fonctionnant uniquement en environnement cryogénique. Cependant les temps de certains calculs effectués par la machine étaient plus importants que ceux obtenus avec un calculateur classique. La société se fixe alors pour objectifs la construction de calculateurs de plus en plus puissants, devants atteindre 1024 qubits fin 2008. Finalement, « seule » une puce de 128 qubits sera présentée en avril 2009. Néanmoins, D-Wave effectuera en 2011 la première commercialisation d'un calculateur quantique, avec la vente d'une machine de 128 qubits à Lockheed Martin, société d'armement américaine. Plus récemment, la société Google s'est associée à la NASA pour un achat d'un calculateur quantique auprès de D-Wave, le but étant d'étudier les apports de l'informatique quantique dans la résolution de problèmes complexes.

Partie 5 : Etat de l'art

5.1) Naissance du calculateur quantique

D-Wave commercialise actuellement l'ordinateur quantique le plus puissant à ce jour, le **D-Wave Two**, puisqu'il s'agit d'un calculateur **512 qubits**.

Cependant, nous ne connaissons pas encore les réelles capacités de cette machine. En effet, rien ne prouve qu'elle évolue dans l'univers quantique. C'est pourquoi la société **Google** (associée à la NASA) s'attèle actuellement à tester leur dernière acquisition, un D-Wave Two, afin de découvrir ce que vaut réellement cette invention…

Une des grandes difficultés rencontrée lors de l'utilisation d'un ordinateur quantique est la lecture du résultat. D'abords, il nous est impossible aujourd'hui de lire les résultats obtenus pour ce genre de calculateur en « **direct** ». Le seul moyen actuel consiste à poser un problème à résoudre au processeur, attendre la résolution, et lire le résultat lorsque le calcul est terminé. Et encore ! Il est même difficile de simplement lire correctement ce résultat ! Puisqu'il est de nature quantique, utiliser les méthodes habituelles fausserait complétement le résultat. Un laboratoire français a pourtant récemment mis au point un algorithme permettant de lire un résultat quantique, et ce avec une fiabilité de **94%**.

L'un des défis lancé depuis la potentielle exploitabilité de l'ordinateur quantique consiste à créer un algorithme capable de « casser » n'importe quel système de cryptographie actuel. La NSA (*National Security Agency*) s'est donc lancée dans cette course technologique, puisqu'un tel algorithme s'avèrerait extrêmement dangereux entre de mauvaises mains (et extrêmement intéressant entre de « bonnes mains »). En effet, les clés de cryptages actuelles sont si longues qu'un ordinateur classique, et même des centaines ne suffiraient pas à en venir à bout. Avec un calculateur quantique, un tel système de cryptage tomberait en quelques minutes. La puissance serait telle que même augmenter la taille de la clé ne servirait à rien... Cependant un tel exploit n'est pas à l'ordre du jour, puisqu'il faudrait pouvoir manipuler plusieurs milliers de qubits à la fois, or le D-Wave Two, rappelons-le, ne fonctionne « qu'en » 512 qubits…

5.2) Hypothèse et prévision

Les ordinateurs construits sur le principe de la physique quantique, à l'opposé de la physique dite classique, promettent une révolution quant à l'évolution du microprocesseur ou de la fission d'un atome.

Plusieurs personnes cherchent encore quelle serait l'utilité d'un ordinateur quantique, en effet, cet instrument d'une monstrueuse capacité est-il simple à gérer ? Nous allons donc vous présenter quelques exemples où un ordinateur quantique serait utile, bien sûr ce ne sont que des prévisions, elles correspondent aussi principalement aux prévisions des D-Waves.

Le **D-Wave one** fut acheté par Lockheed Martin. C'est une entreprise américaine et mondiale de défense et de sécurité. Elle créée et fabrique des véhicules, plus particulièrement des avions mais également des voitures militaires. Grâce à la puissance du D-Wave one l'entreprise souhaiterait tester des logiciels de jets qui permettraient de **sécuriser** les avions, en effet les ordinateurs classiques ne peuvent actuellement pas effectuer ce genre de calculs trop complexes. D'autres utilités pourraient être trouvées au D-Wave :

La découverte de planètes co-existantes avec la Terre. Il est clair qu'avec la puissance de cet ordinateur nous pourrions analyser les informations collectées par les télescopes, satellites et nous pourrions ainsi peut être découvrir des planètes aussi viables que la Terre.

Pour continuer avec des fonctions similaires, il nous serait possible de **détecter le cancer** plus tôt grâce à des statistiques plus précises, nous pourrions ainsi déterminer comment les maladies se développent et cela pourrait à terme sauver plus de vies. Outre la dimension humaine que l'on peut retrouver dans les exemples précédents on peut aussi trouver des exemples plus abstraits mais néanmoins tout aussi intéressants : nous avons parlé de moyens de cryptographie, qui sont évidemment utilisées par tout les grandes institutions financières.

Cependant, il existe des alternatives aux institutions financières : les crypto-monnaies. Le principe d'une crypto-monnaie est d'être basée sur un réseau peer-to-peer, tel que le Bitcoin (le bitcoin est une monnaie virtuelle qui a subit une augmentation financière suppérieure à l'essence, en novembre dernier **1 bitcoin valait 1000$**). Le réseau commun d'ordinateur sécurise les transactions numériques financières du bitcoin, et chaque logiciel gardant des bitcoins (donc de l'argent) crypte cela via une clef de sécurité privé (= identité d'une personne sur le réseau de transaction des crypto-monnaie, dans notre cas) calculatoirement impossible à déchiffrer (ou à « casser »).

Néanmoins, un ordinateur quantique, de part sa puissance de calcul phénoménal, peut venir à bout de cette sécurité, et par conséquent s'attribuer une identité qui n'est pas la sienne, comme par exemple l'identité d'une **place boursière de bitcoin**, et donc obtenir absolument toutes ses ressources. En novembre dernier, l'ensemble des bitcoins pour l'instant en circulation équivalait à une masse de **14 milliards de dollar**. C'est donc une masse d'argent potentielle qu'un ordinateur quantique pourrait subtiliser, en somme

L'ordinateur quantique n'en est donc encore qu'à ses débuts, l'étendue de sa puissance n'étant pas encore exploitable. On notera tout de même l'enthousiasme de la société D-Wave, « leader » sur le marché (puisque seule), quant à la réalisation de calculateurs 1024 qubits, voir même **2048** qubits dans le courant 2015…