2019/2020

L’ordinateur quantique va-t-il remplacer l’ordinateur classique ?

RAPPORT DE VEILLE TECHNOLOGIQUE

CHARLES COGOLUEGNES

Sommaire

Prélude

Cette veille technologique a pour but d'évaluer les évolutions possibles de l'ordinateur quantique, tout en cherchant à savoir si ce dernier pourra remplacer un jour l'ordinateur classique. De ce fait les explications techniques du fonctionnement d'un ordinateur quantique contiennent volontairement des raccourcis. Néanmoins elles restent rigoureuses. Le lecteur se doit d'avoir un bagage scientifique afin de comprendre ce rapport.

Dans un premier temps nous aborderons le fonctionnement global d'un ordinateur quantique. Ensuite nous regarderons dans quelles directions celui-ci pourra évoluer, ainsi que les obstacles qu'il devra franchir. Enfin nous essayerons de le comparer à l'ordinateur classique, en faisant attention a bien donner dans quel contexte.

1) Qu'est-ce qu'un ordinateur quantique

1.1) Le fonctionnement

Alors qu'un ordinateur classique fonctionne avec des bits (0 ou 1), un ordinateur quantique lui fonctionne avec des quantum-bits ou qubits (une superposition entre 0 et 1). En effet le concept de superposition entre 2 états peut nous paraitre assez obscure à notre échelle mais c'est quelque chose d'assez commun dans le domaine de la mécanique quantique. Un processeur quantique utilise donc une particule de ce domaine (photon, électron, etc.). On va pouvoir représenter une certaine proportion de 0 et de 1 en fonction du spin (ou polarisation) de cette particule. Si l'on souhaite prendre une mesure sur un qubit, on va donc le forcer à choisir un état (soit 0 soit 1) et il va donc perdre cette propriété de superposition. Afin d'éviter toute interférence indésirable, le processeur est refroidi à une température proche du zéro absolu. On utilise des micro-ondes afin de communiquer avec un qubit.

On représente un qubit de la manière suivante :

φ |0> + Θ |1> *avec φ et Θ des nombres complexes.*

φ et Θ sont complexes car ils permettent de décrire la position et la direction d'un vecteur Ψ dans une sphère. Par analogie avec une pièce de monnaie, cela permet de d'écrire si la pièce qui tourne est plus ou moins penchée d'un côté.

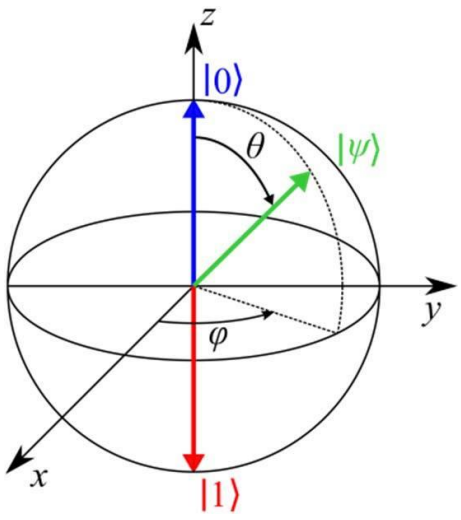

Figure 1 – Représentation de Bloch d'un qubit tiré de researchgate.net

Pour faire simple, nous allons dire qu'un qubit c'est un certain pourcentage (φ) de chance d'avoir 0, plus un certain pourcentage (Θ) de chance d'avoir 1. La somme doit être égal à 1.

Prenons par exemple 3 qubits. Les résultats possibles d'une mesure sur ces 3 qubits sont donc 000, 001, 010, 011, 100, 101, 110, 111. On a 8 résultats possibles ce qui correspond à 2^n états avec n qubits. Cela montre qu'un ordinateur quantique est donc exponentiellement plus rapide qu'un ordinateur classique, car il permet de traiter plusieurs entrées en même temps (on peut dire que c'est une forme de parallélisme).

A ce stade, on peut déjà remarquer qu'un ordinateur quantique va beaucoup plus vite qu'un ordinateur classique. A condition que le nombre de qubits soit suffisamment élevé afin d'observer une différence significative.

1.2) Les opérations quantiques

Comme un ordinateur classique, un ordinateur quantique peut faire passer ses qubits à travers des portes logiques ; qui sont donc quantiques. Il en existe plus d'une quinzaine mais nous allons nous concentrer uniquement sur 2 d'entre elles.

La première est la porte CNOT (Controlled NOT) ou cX. Cette dernière s'applique sur au moins 2 qubits. Elle va tout simplement inverser l'état du second qubit si le premier est égal à |1>. C'est pour cela qu'on dit que c'est une porte avec un qubit de contrôle. Par exemple |00> et |01> restent inchangés, |10> et |11> deviennent respectivement |11> et |10>. Sa représentation schématique est la suivante :

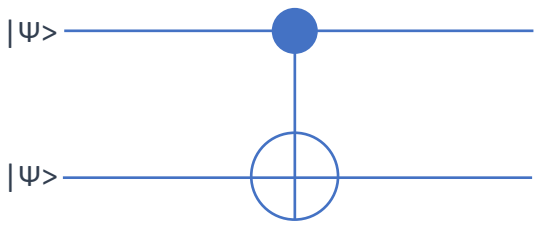

Figure 2 - Porte CNOT

La seconde porte est celle d'Hadamard. Elle permet de passer un qubit étant dans un état propre (|0> ou |1>) dans un état superposé avec une équiprobabilité de devenir 0 ou 1. On a donc pour un qubit q_p dans un état propre, $H(q_p) = 0.5 * |0> + 0.5 * |1>$ (notation simplifiée). Son schéma est le suivant :

Figure 3 - Porte d'Hadamard

Maintenant essayons de les combiner. Prenons 2 qubits étant dans l'état propre |0>. On fait passer le bit de contrôle par la porte d'Hadamard (il est donc en superposition) et on applique un CNOT sur ces derniers.

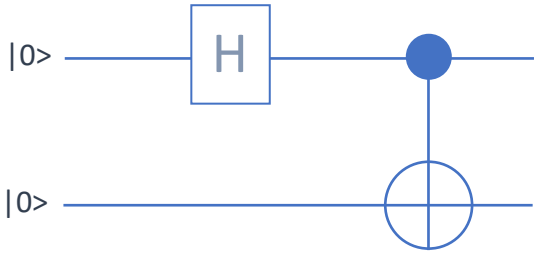

Figure 4 - Intrication de 2 qubits

Désormais nous allons nous intéresser à la matrice A résultante de ces opérations :

$$A = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Cela se démontre en partant du produit tensoriel des matrices $\binom{1}{0}$ pour les 2 qubits puis en appliquant les opérations précédentes (un produit tensoriel entre 2 matrices revient à distribuer la matrice de droite à chaque élément de la matrice de gauche). Ce qui nous intéresse c'est ce qui se passe lorsqu'on essaye de factoriser A afin de revenir au produit tensoriel de départ. On a donc ce système d'équations :

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \binom{a}{b} \otimes \binom{c}{d} \qquad \begin{aligned} ac &= \frac{1}{\sqrt{2}} \\ ad &= 0 \\ bc &= 0 \\ bd &= \frac{1}{\sqrt{2}} \end{aligned}$$

On arrive rapidement à se convaincre que ce système n'a pas de solution.

Ces 2 qubits n'ont donc plus aucun sens de « vivre » séparément. Et pourtant en pratique il est possible de les séparer. Ce phénomène s'appelle l'intrication quantique (entanglement en anglais). Il a pour impact que les 2 qubits vont se corréler (pour ne pas utiliser le terme communiquer) leur résultat lors d'une mesure de l'un d'entre eux. Donc si l'un vaut 1 alors l'autre vaudra forcément 0 (son exact opposé) et inversement. Nous reviendrons plus en détail sur ce phénomène dans la seconde partie.

2) L'évolution possible de l'ordinateur quantique

2.1) Les secteurs propices

Il existe beaucoup de secteurs dans lesquels l'informatique quantique aurait des applications concrètes. Mais on remarque que l'effet bénéfique de ce dernier reste plus ou moins le même. Pour cette raison nous allons nous concentrer sur seulement 2 secteurs.

Le premier est le secteur du médical. Plus particulièrement la simulation de molécules. En effet la modélisation d'atome de certaines molécules doit prendre en compte toutes les interactions possibles entre chaque électron. Ce nombre d'interactions augmente exponentiellement avec le nombre d'atomes, ainsi que le nombre de calcul.

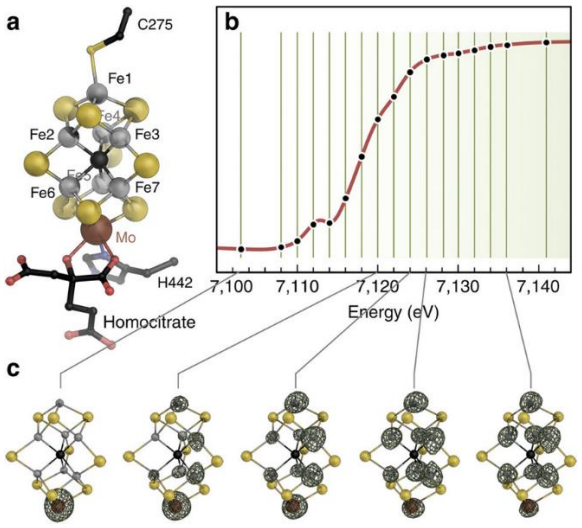

Figure 5 – Différents clusters de la molécule de nitrogénase tirée de researchgate.net

On a vu précédemment qu'un ordinateur quantique était exponentiellement plus rapide qu'un ordinateur classique. Pour cette raison il est capable de gérer dans un temps plus raisonnable les calculs nécessaires. Cela permettrait de découvrir de nouvelles molécules, de nouveaux médicaments et donc faire avancer la médecine en général. De plus cela nous permettrait de mieux comprendre les interactions au niveau microscopique (utiliser un ordinateur quantique pour mieux comprendre les interactions quantiques).

Le second secteur est celui de la cryptographie. Nous verrons par la suite qu'il est intimement lié à celui de la communication, plus particulièrement la sécurité de la communication. Un grand nombre de système de sécurité utilise l'algorithme RSA. Ce dernier se base sur le fait qu'il est extrêmement difficile de factoriser un nombre très grand sous forme de nombres premiers. Par exemple trouver que $5152817 = 2339 * 2203$, dans un temps raisonnable. Il existe des algorithmes classiques permettant de toujours trouver une solution mais leur complexité augmente de manière exponentielle. Un algorithme quantique appelé algorithme de Shor (dont on parlera plus loin) permet lui aussi d'effectuer cette factorisation mais sa complexité augmente de manière logarithmique.

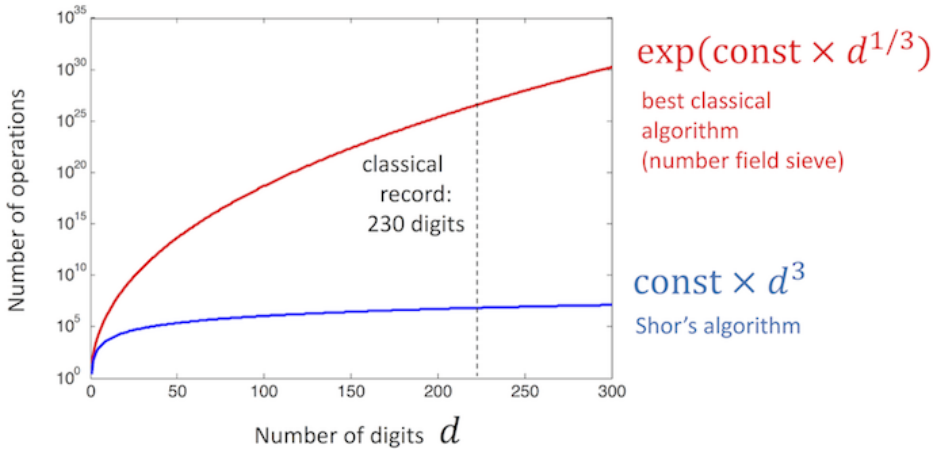

Figure 6 - Algo classique vs algo de Shor tiré du GitHub de Aurélien Pélissier

Un cas de plus où l'on observe la rapidité exponentielle de l'ordinateur quantique. Cet algorithme pourrait donc mettre à mal tous les systèmes de sécurité se basant sur le protocole RSA ? Pour l'instant en pratique ce n'est pas le cas. En effet il faudrait un nombre de qubits assez important afin d'utiliser l'algorithme sur des nombres très grands. A ce niveau nous sommes donc limités par le hardware. De plus, nous verrons par la suite qu'il existe d'autre moyen de communication dit de sécurité absolue grâce à l'informatique quantique.

Nous aurions pu évoquer d'autre secteur tel que l'intelligence artificielle ou encore le domaine de la finance. Mais on s'aperçoit très vite qu'un ordinateur quantique n'est pas très différent d'un ordinateur classique, il va juste beaucoup plus vite à grande échelle. De plus cela n'est valable que pour certain problème, dans un cas comme l'addition par exemple l'ordinateur quantique ne va pas plus vite que le classique (il n'y a pas de différence). Il existe même certaines tâches qu'il n'est pas encore apte à effectuer, comme faire tourner un jeu vidéo ou accéder à Internet par exemple. Nous verrons plus tard les contraintes liés cette rapidité.

2.2) Des exemples concrets

Nous allons désormais parler des applications existantes liées à l'ordinateur quantique. Nous nous intéresserons aussi à quelques algorithmes.

Pour commencer nous allons revenir sur le phénomène de l'intrication quantique. Pour rappel il a pour effet que 2 qubits intriqués donnent un résultat strictement opposé lors d'une mesure

de l'un d'entre eux. Ces 2 qubits ne communiquent pas à proprement parler car cette communication s'effectuerait à une vitesse supérieure à celle de la lumière (violation du principe de causalité). C'est pour cela qu'on dit qu'ils se corrèle leur résultat, car la corrélation elle peut s'effectuait plus vite que la vitesse de la lumière. La théorie des variables cachées par John Bell (physicien du 20ème siècle) permettrait d'expliquer ce phénomène, mais celle-ci est assez controversée.

On voit venir que l'intrication quantique va nous permettre de communiquer. Cette communication est appelée la téléportation quantique (un terme peu révélateur, nous verrons pourquoi par la suite). Nous allons l'expliquer avec un exemple. Prenons 2 personnes Alice et Bob qui ont chacun un qubit. Alice possède un qubit A qui est intriqué avec le qubit B de Bob. Alice souhaite envoyer un autre qubit Q à Bob. Elle va donc intriquer les qubits A et Q et effectuer une mesure sur ces derniers. Elle envoie les 2 résultats des mesures à Bob (par voie de communication classique). Bob va effectuer les opérations suivantes : si le résultat de A est égal à 1 alors il va passer son qubit B par une porte appelée X (qui équivaut à la porte NOT pour un ordinateur classique). Si le résultat de Q est égal à 1 il va passer B par une porte appelée Z (cette porte est légèrement plus complexe et donc ne sera pas détaillée). Ces opérations s'effectuent en série. A la fin Bob va se retrouver avec son qubit B ayant exactement les mêmes caractéristiques que le qubit Q au départ. Voici un schéma récapitulant cet algorithme :

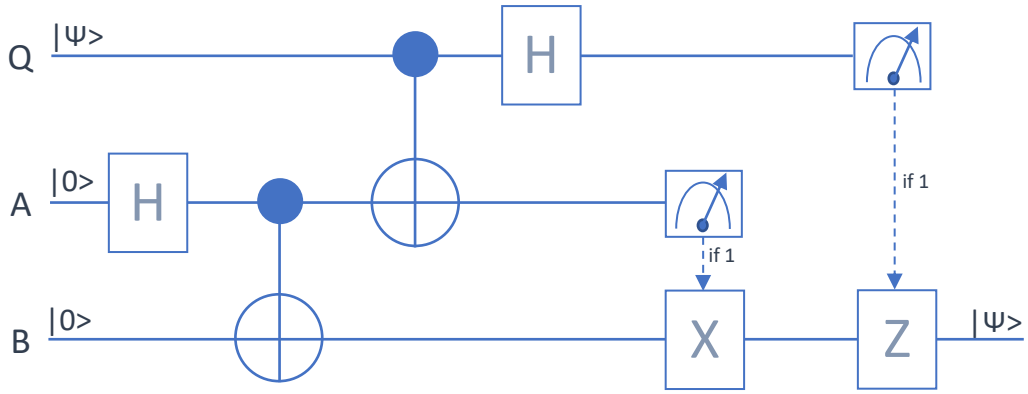

Figure 7 - Schéma téléportation quantique

L'intrication a beau être instantanée, la téléportation elle ne l'est pas. En effet le temps de communication est limité au canal permettant d'envoyer les 2 bits résultants d'une mesure.

Néanmoins, comme évoqué précédemment la sécurité de l'information est absolue. Il est impossible pour une personne tierce d'intercepter l'envoie des 2 qubits intriqués sans effectuer une mesure sur l'une d'entre eux et donc détruire l'état de superposition (pas de copie possible). En 2017, des scientifiques chinois en ont fait la première démonstration depuis l'espace grâce à leur satellite quantique. Ils ont pu ainsi effectuer une mesure sur environ 900 qubits intriqués séparés d'une distance d'environ 1200 kilomètres. Les résultats furent cohérents.

Nous allons poursuivre sur un autre algorithme, celui de Grover (créé par l'informaticien Lov Grover en 1996). Ce dernier permet d'effectuer une recherche clé/valeur dans une base de données non ordonnée. Prenons une valeur y. On souhaite trouver la clé x correspondante à y. On a donc l'équation $f(x) = y$, avec la fonction f que l'on considère comme une boite noire. Une solution classique serait d'essayer les n possibilités de x une par une jusqu'à trouver y. On aura donc au plus n étapes et en moyenne $\frac{n}{2}$ étapes. En regardant une superposition des différents x, l'algorithme de Grover va permettre de déterminer le x ayant la plus grande probabilité de correspondre au y. Il effectuera la recherche en $\sqrt{n}$ étapes.

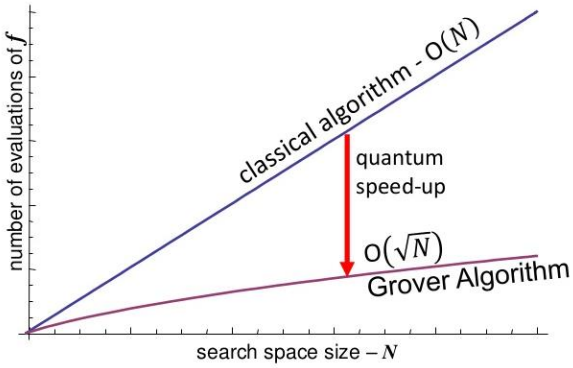

Figure 8 - Comparaison de l'algo de Grover tiré de let's build a quantum computer

Dans un monde où le Big Data prend du plus en plus de sens, où le stockage massif de données devient de plus en plus courant, l'algorithme de Grover peut se révéler très utile. En effet une ressource donnée pourra se trouver stockée sur n'importe quelle base de données et elle ne sera utilisable que si elle peut être retrouvée dans un temps raisonnable.

Un dernier algorithme que l'on peut citer est celui de Shor (crée par le mathématicien Peter Shor en 1994). Cet algorithme évoqué précédemment permet de trouver dans un temps record la factorisation en nombres premiers d'un nombre, très grand si nécessaire. Nous allons dans un premier temps décortiquer un minimum cet algorithme. Enfin nous parlerons de ces applications et de ces limites.

Donc le problème est le suivant : nous avons un nombre entier N, très grand. Nous souhaitons trouver a et b, nombres premiers, tel que $N = a * b$. On commence par choisir au hasard un nombre g. On se donne la formule suivante : $g^p = m * N + 1$, avec p et m des nombres entiers. En français, cela veut dire que si l'on multiplie notre nombre g par lui-même p fois, alors nous allons trouver un nombre qui est égal à un multiple de N plus 1. Grâce à l'algorithme d'Euclide, nous pourrons alors retrouver notre nombre N. Une fois g trouvé, disons que $a = g$, il est alors possible de trouver $b = \frac{N}{a}$.

D'apparence, on peut penser que cet algorithme peut s'effectuer sur un ordinateur classique, et c'est vrai. Mais plus le nombre N est grand, plus le temps de calcul devient aberrant (c'est sur quoi se base la sécurité de nos transactions aujourd'hui). On va donc le faire tourner sur un ordinateur quantique. Mais là un autre problème apparait : le fait de faire passer nos différents g en superposition nous amène à avoir une transformation qui donne elle aussi une sortie en superposition. Lorsqu'on effectue une mesure sur cette sortie nous allons donc avoir un résultat qui sera tiré au hasard, et donc qui ne correspondra pas forcément à ce que l'on attend. En bref, il serait possible d'avoir par exemple ce résultat : $g^p = m * N + 42$. Pour le résoudre nous allons utiliser la propriété de répétition de cette formule. En effet, on remarque la chose suivante : si $g^x = m_1 * N + r$ alors $g^{x+p} = m_2 * N + r$, avec x et r des nombres entiers. On observe alors la périodicité p de cette série. On va donc utiliser la transformée de Fourier quantique afin de trouver la fréquence $f = \frac{1}{p}$. Et voilà, nous avons trouver p et nous pouvons effectuer le reste des calculs (il faut savoir que beaucoup de choses ont été simplifiés dans cette explication).

En réalité avec les ordinateurs quantiques actuels, le plus grand nombre que nous avons réussi à factoriser est 291311. Pour un nombre contenant quelques centaines de chiffres (ce genre de nombre est utilisé dans les algorithmes de chiffrement actuels), il faudrait entre 5000 et 6000 qubits. Pour l'instant nous en sommes à une cinquantaines.

2.3) La suprématie quantique

La suprématie quantique est un terme inventé par John Preskill (physicien américain) qui désigne le jour où un ordinateur quantique arrivera à résoudre un problème qu'un ordinateur classique n'est pas capable de résoudre dans un temps raisonnable.

Nous allons parler de ce terme car, en apparence, il semble marqué la fin des ordinateurs classiques au profit des ordinateurs quantiques. Nous verrons qu'en réalité ce n'est pas du tout le cas.

En octobre 2019, Google a annoncé avoir franchi cette barrière. En effet avec leur processeur quantique nommé Sycamore de 53 qubits, ils ont réussi à résoudre un problème en 200 secondes alors qu'il aurait fallu environ 10 000 ans à un ordinateur classique. Le problème en question est l'échantillonnage d'un circuit quantique. Il ne s'agissait pas d'un problème majeur mais la démonstration fut suffisante pour affirmer que la suprématie quantique était atteinte.

Cette démonstration a été très controversée notamment par IBM (concurrent direct de Google). IBM a prouvé qu'avec leur supercalculateur, et avec quelques optimisations de l'algorithme, il pourrait résoudre ce problème en seulement 3 jours. De ce fait IBM pense que la démonstration de Google n'est pas valide et que la suprématie quantique n'a pas encore été atteinte.

Nous allons analyser les arguments des 2 partis et nous allons en tirer des conclusions. Certes le problème choisi par Google n'est pas très utile en soi. Mais à la base c'est le terme de suprématie qui est mal choisi. En effet cela évoque un sentiment de domination et de puissance, des termes qui sont totalement hors contexte avec le sujet. Par conséquent IBM a cherché à réduire cet engouement en montrant que le problème pourrait être résolu en beaucoup moins de temps. D'une part IBM suppose qu'il faudrait 3 jours à leur supercalculateur pour résoudre le problème, ils ne l'ont pas réellement testé. La raison est que l'algorithme modifié demande énormément d'espace de stockage (quasiment la totalité de la mémoire du supercalculateur). D'autre part l'argument semble bancale si l'on ajoute le fait qu'un seul qubit en plus dans le processeur suffirait à surpasser le supercalculateur avec un facteur de 100. L'argument ne sera donc plus valable à la prochaine démonstration. Pour finir, même s'il l'on se base sur les chiffres actuels, le processeur quantique de Google va tout

même plus de 1000 fois plus vite que le supercalculateur d'IBM utilisé à 100 %. Un facteur qui n'est pas insignifiant.

Pour conclure, on peut dire que Google a bien atteint cette suprématie quantique. C'est le terme de suprématie qui n'est pas adapté. Enfin, il faut dire qu'IBM a des arguments tout à fait légitimes pour l'instant, mais ces derniers ne seront plus valables dans quelques années.

3) Les freins à ce développement

3.1) La décohérence quantique

La décohérence quantique est un phénomène (découvert par le physicien Dieter Zeh en 1970) se produisant sur une particule en superposition. Si cette dernière est dans un endroit chaud et éclairé par exemple, elle va interagir avec les autres particules présentes dans le milieu. Celle-ci va donc perdre sa propriété de superposition (c'est pour cela qu'un processeur quantique est très bien isolé et refroidi proche du 0°K). De plus, même si les qubits de ce processeur sont extrêmement bien « protégés », ces derniers vont quand même interagir entre eux et perdre leur propriété de superposition à un moment donné. Le temps requis afin de préserver cette cohérence est en général de l'ordre du nano ou microsecondes. En d'autre termes, la décohérence est l'effet produit à la frontière entre le monde dans lequel nous vivons et celui du quantique.

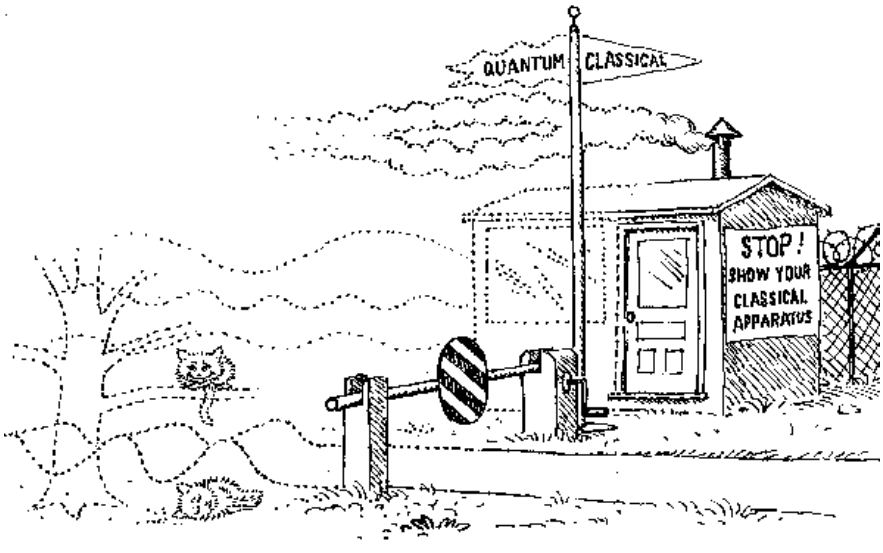

Figure 9 - Dessin de la limite entre monde macro et quantique tiré de iqst

C'est donc un des grands défis de l'informatique quantique, réussir à maintenir les qubits en cohérence. A l'heure actuelle, le temps maximum qu'a réussi à tenir un qubit en superposition dans une pièce à température ambiante est de 39 minutes (voir l'article). Il faut préciser que le taux de fidélité du qubit n'était que de 81 %.

3.2) L'évolution du nombre de qubits par année

Nous avons vu précédemment qu'un des meilleurs processeurs quantiques actuel contient environ 53 qubits. Prenons un objectif de 300 qubits à atteindre (on parle ici de qubits supraconducteurs à base de porte quantique). Si ces qubits sont parfaitement intriqués, cela permettrait entre autres de simuler toutes les interactions dans l'Univers jusqu'à ces débuts.

Cela est très compliqué voire impossible d'estimer l'évolution du nombre de qubits chaque année. La raison est que nous ne connaissons pas la nature de cette évolution. Est-elle exponentielle, linéaire, logarithmique ? Le fait que des gouvernements investissent plusieurs milliards de dollars dans la R&D de l'informatique quantique nous amène à pense que cette évolution ne peut que s'accélérer.

On va donc se baser sur une évolution de 3 qubits par an. Ce chiffre reste raisonnable et n'est probablement pas surestimé. On arrive donc à une durée d'environ 50 ans afin d'atteindre cet objectif. Il faut préciser que cette durée est une durée maximale et qu'il n'est pas impossible d'atteindre 300 qubits dans les 20 prochaines années.

3.3) Mesures imprécises et stockage difficile

Pour rappel, lorsqu'on effectue une mesure sur un qubit on le force à choisir un état. Prenons un qubit q et faisons-le passer par une série de porte quantique P. A la fin on effectue une mesure sur q et on s'attend à avoir le même résultat à chaque fois qu'on le fait passer par P. En réalité, lorsqu'on échantillonne ce circuit, on remarque un certain taux d'erreur ressortant comme du bruit. Pour un processeur comme Sycamore ce taux d'erreur est de 2%. De plus, à chaque passage d'une porte quantique, on observe un taux d'erreur additionnel de 0.2%. Donc plus le nombre de portes augmente plus l'erreur sera significative.

Une première solution serait d'effectuer ces opérations un certain nombre de fois afin d'obtenir un taux de fidélité assez important pour en tirer des conclusions. Cette dernière est tout à fait plausible car même en répétant n fois un procédé sur un problème, l'ordinateur

quantique reste plus rapide que le classique. Mais nous voyons bien qu'elle n'est pas viable dans le temps.

Une autre solution serait d'améliorer le processeur quantique afin qu'il fasse moins d'erreur. Cette solution reste de loin la meilleure mais par conséquent la plus compliqué à réaliser. C'est pour cela qu'il existe une troisième solution qui est une sorte de compromis. On va utiliser des codes correcteurs d'erreurs (comme sur les ordinateurs classiques) afin de corriger les résultats faussés. Cette solution est viable car il existe déjà des algorithmes quantiques correcteurs d'erreurs. Le seul problème c'est qu'il faut un nombre de qubits importants (cela explique les milliers de qubits nécessaires pour l'algorithme de Shor). On en revient donc au fait que nous sommes limités par l'évolution du nombre de qubits.

Le stockage de qubits est un autre problème. En effet a l'heure actuelle il est impossible de stocker de l'information quantique pour une durée acceptable. Le record est actuellement de 30 secondes avec un taux de fidélité supérieur à 99.99 % (voir l'article). En effet juste stocker un qubit n'est pas suffisant. Il faut que l'on puisse le retrouver exactement dans l'état dans lequel nous l'avons laissé. Un autre obstacle à surmonter.

4) Conclusion

Dans cette conclusion, je vais donner un avis personnel afin de répondre à la problématique. J'utiliserai la première personne pour exprimer mes arguments. La réponse apportée ne sera donc pas universelle, elle sera strictement personnelle.

4.1) La plus-value d'un ordinateur quantique

Nous avons vu tout au long de ce rapport que l'avantage principal d'un ordinateur quantique est sa rapidité exponentielle. Celle-ci engendre donc des applications très prometteuses dans les différents secteurs évoqués.

Il en existe d'autres. Par exemple le fait qu'un ordinateur quantique est beaucoup moins gourmand en énergie qu'un ordinateur classique, à nombre d'opérations égales. En effet l'ordinateur classique va devoir stocker un grand nombre de résultats afin de simuler le phénomène de superposition. Cela engendre donc une infrastructure et une consommation plus importante.

4.3) L’ordinateur quantique complémentaire à l’ordinateur classique

Je pense que la comparaison entre l’ordinateur quantique et l’ordinateur classique n’est pas très juste. Cela reviendrait à comparer par exemple une bougie à une lampe allogène. Certes la fonction est basiquement la même mais la technologie derrière est totalement différente. De plus nous sommes encore en phase expérimentale sur l’ordinateur quantique. Il est donc facile d’effectuer des spéculations assez élogieuses sur ces évolutions possibles.

Si l’on se base sur les décennies à venir, je pense que l’ordinateur quantique n’aura pas totalement remplacé l’ordinateur classique. Néanmoins il est tout à fait possible que les 2 travaillent ensemble. Par exemple, j’imagine très bien un ordinateur classique effectuer une requête sur un serveur possédant un processeur quantique. L’idée étant d’accélérer les calculs qui pourront lui prendre du temps, et donc améliorer l’expérience utilisateur en général.

En ce qui concerne les entreprises, je pense qu’il est indispensable pour elles d’effectuer une veille sur l’informatique quantique. Surtout si la sensibilité de leurs données est élevée. En effet les mesures à prendre afin de palier à ce problème doivent être effectuer bien en amont.

Pour finir, mis à part la sécurité de leurs données, l’efficacité en termes de temps calcul n’est pas négligeable et donc il est à prendre en compte. Un investissement dans le domaine est donc vivement conseillé.

Table des figures

Références

Quantum Computing for Computer Scientists, *Andrew Helwer*, Microsoft.

A beginner's guide to quantum computing, *Shohini Ghose*, Ted.

La suprématie Quantique de Google, *David Louapre*, Science Etonnante.

A Beginner's Guide to Quantum Computing, *Talia Gershon*, IBM Research.

Quantum Computing Explained in 5 Levels, *Talia Gershon*, Wired.

Les Ordinateurs Quantiques, *David Louapre*, Science Etonnante.

Quantum Teleportation From Space Achieved by China, *Dagogo Altraide*, ColdFusion.

Shor's Algorithm Explained, *Henry Reich*, minutephysics.

Les origines de la décohérence quantique, *Michel Brune*, Ecole normale supérieure – PSL.

La Décohérence quantique, *Alessandro Roussel*, ScienceClic.