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.

# Qu’est-ce qu’un ordinateur quantique

## 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 qubits, 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 Ѱ 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.

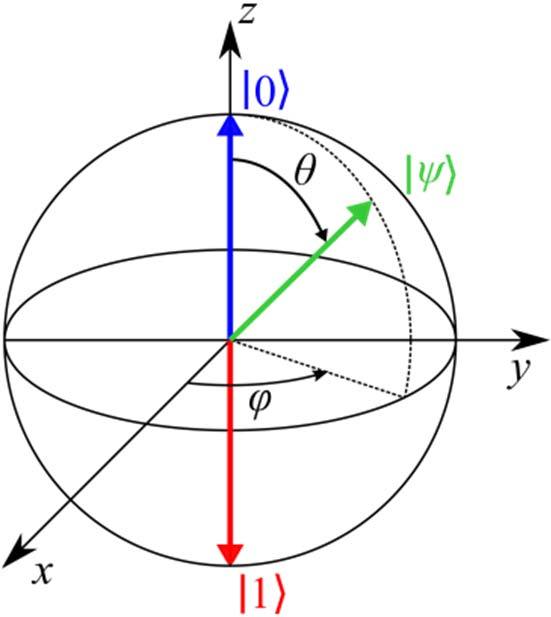


Figure 1 – Représentation de Bloch d’un qubit tiré de <researchgate.net>

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 2n états avec n qubits. Cela montre qu’un ordinateur quantique est donc exponentiellement plus rapide qu’un ordinateur classique.

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.

## 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 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 :

|Ѱ>

|Ѱ>

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 qp dans un état propre H(qp) = 0.5 \* |0> + 0.5 \* |1> (notation simplifiée). Son schéma est le suivant :

|Ѱ>

H

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.

|Ѱ>

H

|Ѱ>

Figure 4 - Intrication de 2 qubits

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

A =

Cela se démontre en partant du produit tensoriel des matrices 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). Mais 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 :

*ac =*

= ⊗

*ad = 0*

*bc = 0*

*bd =*

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 (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 1 et inversement. Nous reviendrons plus en détail sur ce phénomène dans la seconde partie.

# 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.

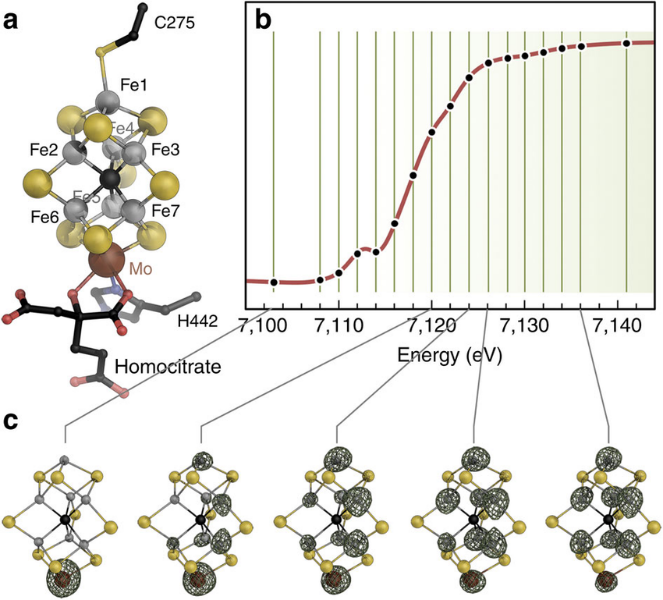


Figure 5 – Différents clusters de la molécule de nitrogénase tirée de <researchgate.net>

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 la cryptographie. Nous verrons par la suite qu’il est 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 grand nombre sous forme de nombre premiers. Par exemple trouver que *5152817 = 2339 \* 2203* dans un temps raisonnable. Il existe des algorithmes classiques permettant de toujours trouver une solution mais sa 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.

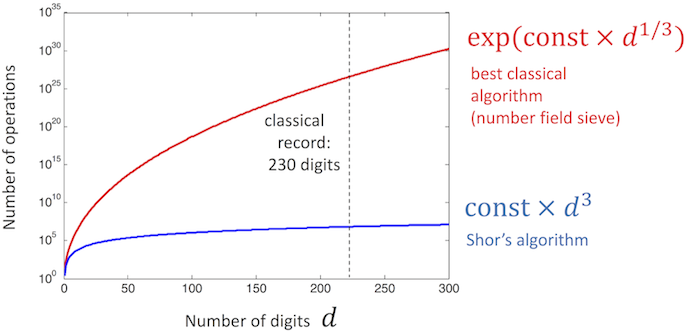


Figure 6 - Comparaison entre algo classique et algo de Shor tiré du [GitHub](https://github.com/Aurelien-Pelissier/IBMQ-Quantum-Programming) de Aurélien Pélissier

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 des 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 existe même certaines tâches qu’il n’est pas encore apte à effectuer, comme faire tourner un jeu vidéo par exemple. Nous verrons plus tard les désavantages à 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 le même résultat. 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. Alice va donc intriquer les qubits A et Q et effectuer une mesure sur ces derniers. Alice 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 :

Q

|Ѱ>

X

H

H

if 1

|0>

if 1

A

B

|Ѱ>

|0>

Z

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).

Nous allons poursuivre sur un autre algorithme…

<<Parler de algo Grover + Shor>>

## 2.3) La suprématie quantique

La suprématie quantique est 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 cabale de résoudre dans un temps raisonnable.

# Les freins à ce développement

## 3.1) La décohérence quantique

## 3.2) L’évolution du nombre de qubits par année

## 3.3) Mesures imprécises et stockage difficile

# Conclusion

## 4.1) La plus-value d’un ordinateur quantique

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