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 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). Afin d’éviter toute interférence indésirable, le processeur est refroidi à une température proche du zéro absolu.

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.

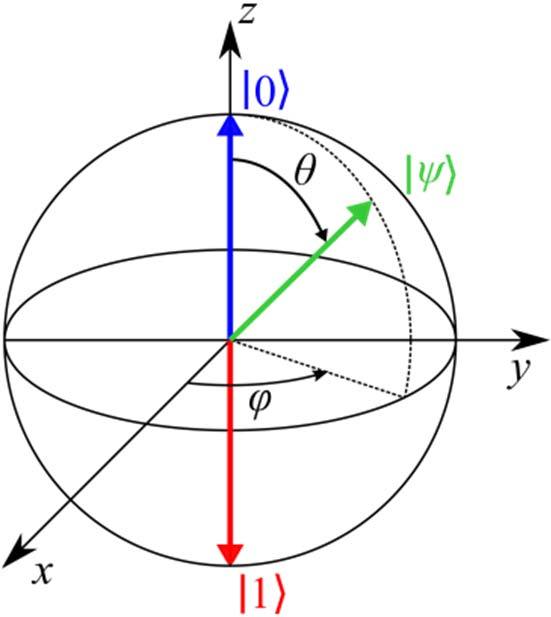


Figure – Représentation d’un qubit tiré de <researchgate.net>

Pour faire simple, un qubit c’est un certain pourcentage (ϕ) de chance d’avoir 0, plus un certain pourcentage (ϴ) de chance d’avoir 1. Le tout 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 - 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 - 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 - 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 plus 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

## 2.2) Quelques algorithmes

## 2.3) La suprématie quantique

# Les freins à ce développement

## 3.1) La décohérence quantique

## 3.2) Un grand nombre de qubits requis

# Conclusion

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

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