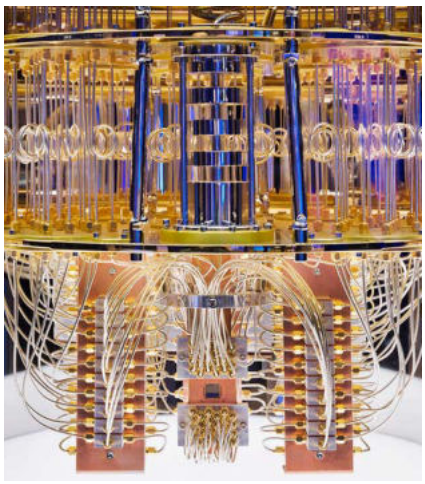


NUMERO SPÉCIAL
octobre 2021

Introduction
à
l'ordinateur
quantique

UNE INTRODUCTION A L'ORDINATEUR QUANTIQUE

On entend de plus en plus parler de l'ordinateur quantique dans les médias, mais sans vraiment comprendre de quoi il s'agit.
Ne vous inquiétez pas, ce n'est pas votre faute : l'informatique quantique est un domaine un peu complexe à première vue. Mais grâce à cet article, vous découvrirez :

- Pourquoi on a vraiment besoin des ordinateurs quantiques
- Pourquoi ils font un peu peur quand même
- Comment fonctionnent des algorithmes quantiques
- Les notions de bases en physique pour comprendre leur fonctionnement ;

Et les réponses des grandes questions comme : est-ce qu'on va bientôt tous avoir notre ordinateur quantique dans le salon ?
Avant de commencer, vous devez être sûr(e) de comprendre le fonctionnement de base d'un ordinateur normal.
Ça fait quoi, un ordi pas quantique ?

Même si on a l'impression qu'un ordi fait plein de choses, en réalité, il n'a qu'une seule mission : il traite de l'information (d'où le mot "*informatique*").

Votre ordinateur stocke de l'information sur votre disque dur, il traite des info avec son processeur (comme la page que vous lisez ou un film que vous regardez), et il transforme cette information en un son (dans vos haut-parleurs) ou en image (sur votre écran). Point final.

Cette information que manipule l'ordinateur a la caractéristique d'être codée en binaire, c'est-à-dire avec des 0 et des 1. Autrement dit, un ordinateur « réfléchit » en binaire.

Une mémoire d'ordinateur est ainsi constituée de milliards de cases contenant soit un 0, soit un 1. Une telle case s'appelle un *bit*. Pour manipuler ces bits, votre ordinateur est rempli de petits composants électroniques qui travaillent ensemble et que l'on appelle "des portes logiques".

```
01110011 01100101 01110010 01
01100101 01110010 00100000 01
01101000 01100001 01110100 00
01100100 01101001 01110011 01
01110010 01101001 01100010 01
01110100 01100101 01110011 00
01100001 01101110 01111001 00
01101001 01101110 01100011 01
01101101 01101001 01101110 01
00100000 01101101 01100101 01
```

➔

➔ Pour être utilisable par un ordinateur, le code d'un programme quelconque doit être encodé en binaire,

Mais votre ordinateur ne peut pas résoudre tous vos problèmes ! On a l'impression que les ordinateurs peuvent résoudre tous les problèmes du monde parce qu'ils sont puissants et efficaces. Et c'est faux !

Les chercheurs rencontrent souvent des problèmes que leurs ordinateurs ne peuvent pas résoudre. Alors, ils cherchent des moyens de rendre leurs ordi plus puissants. Pour rendre un ordinateur *plus puissant*, il faut :

- augmenter sa mémoire (pour stocker + d'informations).
- augmenter le nombre de transistors dont il dispose (pour traiter + d'informations).

Malheureusement, il arrive un moment où **r**ajouter de la mémoire et du processeur ne suffit même plus à rendre l'ordi satisfaisant.
Car même les meilleurs supercalculateurs (des ordi géants, utilisés par les chercheurs) peuvent être surmenés par certains problèmes résolument trop compliqués. Ces ordinateurs ne sont pas faits pour résoudre ces problèmes complexes. Ils ne "pensent" tout simplement pas de la bonne manière.

Un supercalculateur chez IBM. Il fonctionne à peu près comme votre ordinateur à vous – avec des processeurs et de la mémoire – sauf qu'il intègre des dizaines de milliers de processeurs (alors que le votre n'en possède généralement que 2, 3 ou 4).

Ces super-ordi, aussi puissants soient-ils, sont donc dépassés par certains problèmes. D'où l'idée d'un ordinateur quantique qui aurait un fonctionnement tout à fait différent. Les premières théories de l'informatique quantique sont nées dans les années 80, et utilisent des propriétés étonnantes de la physique quantique.

Deux phénomènes au cœur de l'ordinateur quantique

Pour comprendre le fonctionnement d'un ordinateur quantique, pas de mystère : vous devez déjà comprendre les bases de la physique quantique. Voyons 2 notions essentielles, le plus simplement possible.

1. La superposition quantique

Au début du XXe siècle, les physiciens se sont rendu compte du fait que la matière se comportait bizarrement dans l'infiniment petit. Par exemple, une particule de l'infiniment petit peut se trouver dans un état indéterminé avant toute mesure.

On peut faire une analogie avec un ticket de loterie : un ticket de loterie est soit gagnant, soit perdant. Une fois qu'on regarde le résultat du tirage à la télé, on a la réponse. Mais avant le tirage, ce ticket n'était ni gagnant, ni perdant. Il avait simplement une certaine probabilité d'être gagnant et une certaine probabilité d'être perdant.

Dans le monde quantique, toutes les caractéristiques des particules peuvent être sujettes à cette indétermination : par exemple, la position d'une particule quantique est incertaine : elle n'est pas à un point A ou un point B, mais a seulement une probabilité d'être ici ou là lors d'une mesure. Avant la mesure, la particule n'est ni au point A, ni au point B. Par contre, après la mesure, l'état de la particule est bien défini : elle est au point A ou au point B.

Cette indétermination est une idée qui était absolument novatrice pour les physiciens du début du XXème siècle. En effet, en physique classique, l'état d'un objet est toujours défini.

Prenons l'exemple d'un jeu de pile ou face et imaginez que vous lancez une pièce en l'air. Avant de regarder le résultat, vous savez qu'il y a une chance sur deux pour que la pièce tombe sur pile, et une chance sur deux que la pièce tombe sur face. Avant de faire une mesure (c'est à dire de regarder la pièce), vous ne savez pas quel est son état, mais celui-ci est bien défini : soit pile, soit face. Le fait de regarder la pièce ne va rien changer à son état.

Si la pièce était quantique, il en serait différemment : avant de regarder, la pièce aurait un état indéfini, et c'est la mesure qui la placerait soit dans un état, soit dans l'autre.

Bizarre, non ?

Tenter d'expliquer la physique quantique avec des objets du quotidien pose des gros problèmes, c'est ce qu'a essayé de faire comprendre Schrödinger ***avec sa fameuse expérience du chat de Schrödinger*** (que vous devriez absolument découvrir pour mieux comprendre).

2. L'intrication quantique

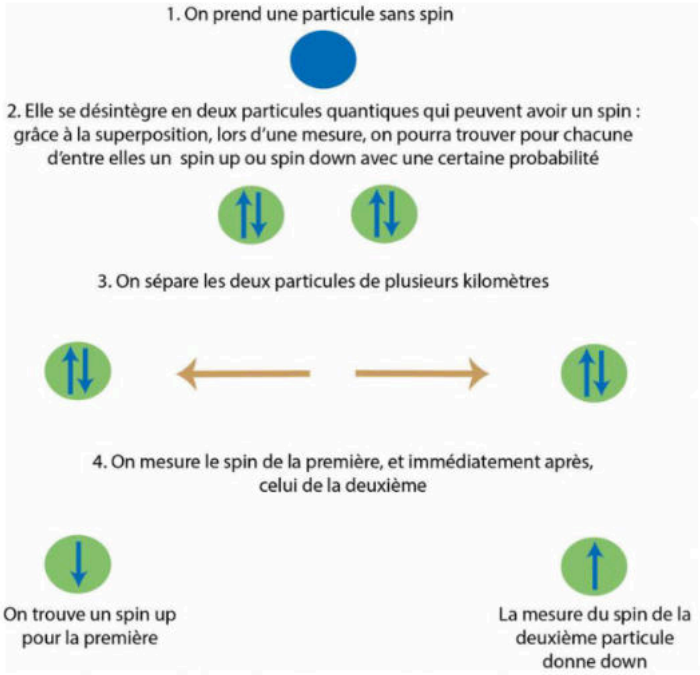
L'intrication est une autre propriété étonnante de la physique quantique. On peut lier deux objets quantiques a priori indépendants : par exemple, on peut les forcer à être dans des états opposés au moment d'une mesure.

Pour illustrer ça naïvement, imaginez 2 ampoules, chacune dans deux maisons différentes. En les intriquant, il deviendrait possible de connaître l'état d'une ampoule (allumée ou éteinte) en observant simplement la seconde, car les deux seraient liées, intriquées.

Revenons à la physique. Certaines particules microscopiques ont une propriété appelée *le spin*. Il n'est pas nécessaire de savoir de quoi il s'agit exactement (mais si vous êtes curieux, voyez la ***page wiki***). Si besoin, pensez à cela : vous êtes caractérisé-e, entre autre, par la couleur de vos cheveux. Cette couleur peut valoir "brun", "roux", "blond". Bref, c'est l'une de vos caractéristiques. Et bien une particule, elle, est caractérisée par son "spin", peu importe ce que c'est.

Tout ce que vous devez savoir, c'est que si une particule a un spin, il ne peut valoir soit *up*, soit *down*. Imaginons maintenant l'expérience suivante :

➔



On pourra mesurer le spin de la première particule des centaines de fois : si ce spin est "up", alors le spin mesuré pour la deuxième particule **s**era toujours son opposé ("down"). Et vice versa !

Comment deux particules, éloignées de plusieurs kilomètres, pourraient-elles se "mettre d'accord" en se transmettant une information, pour toujours être dans un état opposé l'une de l'autre ?!

Là... c'est la panique pour les physiciens, parce que la théorie de la relativité nous enseigne qu'aucune information ne peut être transmise à une vitesse supérieure à celle de la lumière (c'est le ***paradoxe EPR*****)**.

Pour résoudre ce paradoxe, il faut accepter le fait que les deux particules, malgré leur séparation spatiale de plusieurs kilomètres, ont continué à former un unique système physique. En fait, aucune information n'a été échangée entre les deux particules, tout simplement parce que les deux particules ne forment pas deux systèmes indépendants mais un seul. On parle alors *d'intrication quantique*.

On peut intriquer 3 particules ensemble, et même beaucoup plus ! Ce qui est important à retenir est le fait qu'en physique quantique, on peut lier plusieurs systèmes qui semblent indépendants et éloignés, voire extrêmement éloignés.

Si vous avez envie (et besoin) de mieux comprendre ce phénomène frappant, allez voir le super article sur la ***théorie des variables cachées*****.**

Maintenant que vous connaissez les bases de la physique quantique, on va pouvoir parler de l'ordinateur quantique !

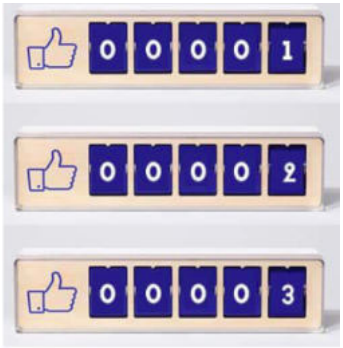
Quel est le principe d'un ordinateur quantique ?

La base de tout : le qbit (à prononcer "kubite")

Au lieu d'utiliser des bits qui ne peuvent prendre comme valeur que 0 ou 1, l'ordinateur quantique utilise des bits quantiques, ou qbits, qui ne prennent pas comme valeur 0 ou 1, mais une superposition de 0 et de 1.

Imaginez un défi un peu bête : utilisez le compteur ci-dessous pour m'afficher tous les nombres qui existent entre 0 et 99999 :

Vous n'aurez pas d'autres choix que de passer par toutes les combinaisons pour réussir ce défi :



...

C'est exactement comme ça que fonctionne un ordinateur classique pour compter. Il doit traiter chaque information, chaque "nombre" dans notre exemple, une à une.

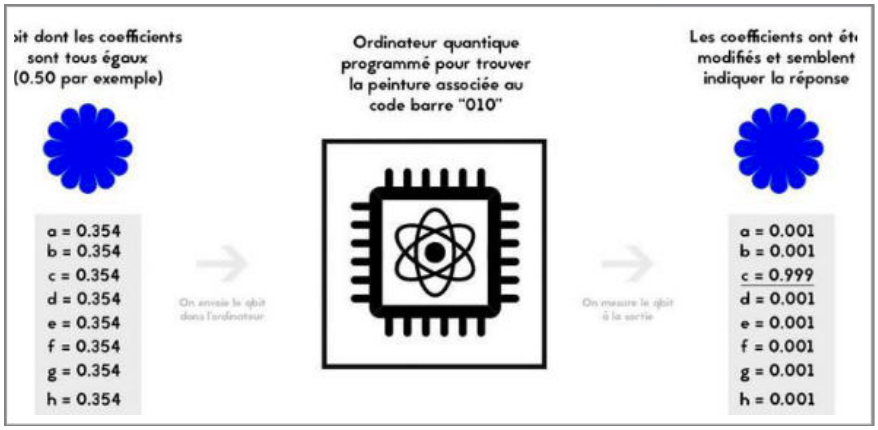
Un ordinateur quantique va raisonner autrement. Voila comment un ordinateur quantique réagirait si je le mettais au défi :

Le principe, c'est celui de la superposition quantique qu'on a vu plus haut. Une case du compteur, autrement dit 1 bit, ne représente plus une seule valeur comme on en a l'habitude, mais une superposition de plusieurs valeurs **(** 9 dans notre exemple.)

➔

➔ Que cet exemple du compteur ne vous trompe pas : en informatique quantique, un ordinateur continue à travailler avec des 0 et des 1. L'ordinateur quantique ne superpose non pas 9 valeurs comme le fait le compteur ci-dessus, mais seulement 2 valeurs (0 et 1).

Ça reste un exploit. Concrètement, cela veut dire qu'un ordinateur quantique peut calculer beaucoup plus rapidement qu'un ordinateur classique, puisqu'il peut traiter tous ses états possibles en même temps (pour reprendre l'analogie du compteur : il a compté en 1 fois au lieu de compter 99999 fois).



Un ordinateur quantique à 4 qbits va calculer 16 fois plus rapidement qu'un ordinateur classique à 4 bits, et ainsi de suite. On double la puissance d'un ordinateur quantique à chaque fois qu'on lui ajoute un qbit ! Ce qui n'est pas le cas pour un ordinateur classique.

*En juillet 2021, un ordinateur contenant l'un des processeurs Falcon à **27 qubits** d'IBM, a été mis à la disposition des scientifiques.*

Comment fonctionne un algorithme quantique ?

Un des algorithmes quantiques particulièrement prometteurs en informatique quantique est l'algorithme de Grover, qui permet de trouver un élément dans une liste : un numéro de téléphone associé à un nom, le code-barre associé à un produit, ou n'importe quel élément dans un gros jeu de données.

Imaginez que vous ayez un magasin de peinture qui vende 8 produits différents, chacun doté d'un code :

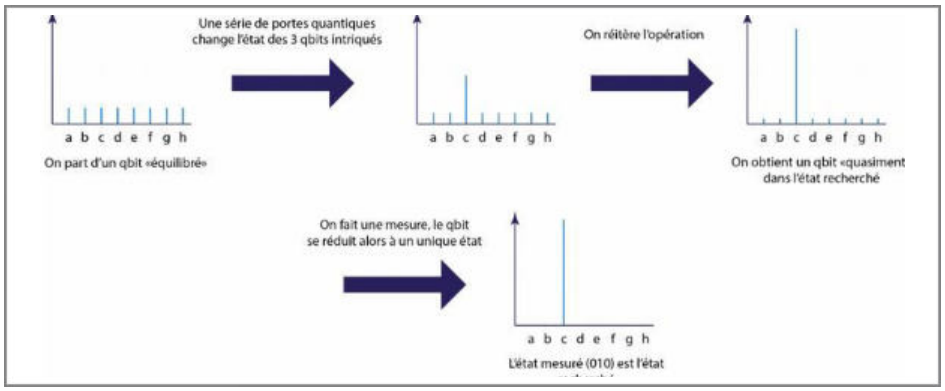
- Peinture rouge : 000
- Peinture jaune : 001
- Peinture bleue : 010
- Verte : 011, rose : 100, magenta : 101, marron : 110, noire : 111

On cherche à savoir quelle est la couleur associée à tel ou tel code-barres de manière automatisée. Évidemment ça paraît absurde tellement le catalogue de peinture est petit, mais imaginez la même situation avec 5000 couleurs et 5000 code-barres !
Vous décidez de résoudre le problème avec la physique quantique ! Vous créez un ordinateur quantique à 3 qbits, qui se trouvent donc avant toute mesure dans une superposition de 8 états différents, chacun correspondant à une peinture. Autrement dit :

- Peinture rouge : correspond au coefficient **a**
- Peinture jaune : correspond au coefficient **b**
- Peinture bleue : correspond au coefficient **c**
- Verte : **d**, rose : **e**, magenta : **f,** marron : **g**, noire : **h**

a(000) + b(001) + c(010) + d(011) + e(100) + f(101) + g(110) + h(111)

Vous créez un circuit de portes quantiques qui a la caractéristique « d'augmenter » le coefficient associé à la peinture recherchée.
Voyons ça en dessin, ça sera sûrement plus intuitif :
Une fois l'ordinateur programmé, on lui "envoie" un qbit neutre dont les coefficients sont égaux.
Après avoir fait plusieurs tours dans le circuit de l'ordinateur, ce qbit va ressortir dans un état superposé, mais avec le coefficient lié à la peinture recherché bien plus élevé que les autres. Lorsque l'on fait une mesure, on peut théoriquement tomber sur n'importe quel état, mais comme le coefficient associé à un état reflète la probabilité de tomber sur cet état



lors de la mesure, on tombe avec une quasi-certitude sur le bon état.
Ainsi les algorithmes quantiques sont souvent probabilistes : ils ne renvoient pas la bonne réponse à coup sûr, mais on peut faire en sorte qu'ils donnent la réponse avec une probabilité très proche de 1.

L'ordinateur quantique a des limites

1 - La réduction du paquet d'onde

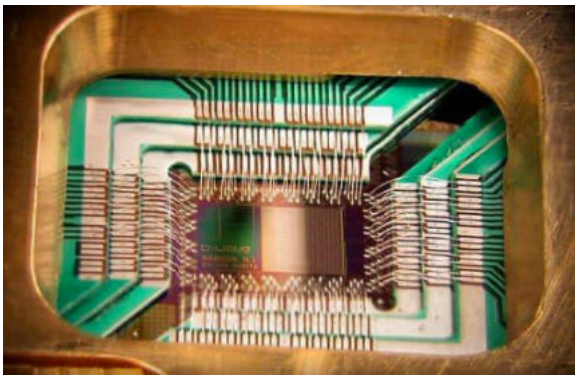
Nous avons vu que les qbits pouvaient contenir beaucoup plus d'informations que des bits classiques, avec coefficients qui entrent en jeu pour n qbits. Le problème, c'est qu'il est très difficile (pour ne pas dire impossible) d'avoir accès à ces coefficients. Ce qu'il faut comprendre, c'est que l'ordinateur quantique va effectuer ses calculs en utilisant les spécificités de la physique quantique (superposition, intrication). Ça permet des calculs complexes.
Mais lorsqu'on lit le résultat d'un calcul quantique, il se passe ce qu'on appelle un effondrement quantique.

➔

➔ Autrement dit, le système quantique perd son caractère quantique lorsqu'on effectue une mesure.

Pour reprendre l'analogie du ticket de loterie : le ticket devient soit gagnant, soit perdant lorsqu'on découvre le résultat. Il perd sa faculté à être l'un et l'autre à la fois.

En particulier, la capacité quantique des n qbits "d'enregistrer" 2^n coefficients disparaît, et les qbits deviennent des bits classiques de valeur 0 ou 1.
Ainsi, le résultat de l'opération qu'effectue le calculateur quantique doit pouvoir être contenu dans n bits seulement. L'utilisation des 2^n coefficients ne sert que d'intermédiaire pour le calcul.



puce d'un ordinateur quantique (D-Wave systems)

2 - Le théorème de non-clônage des qbits

L'ordinateur quantique connaît d'autres limites
Une opération classique en informatique est la copie. Lorsque vous copiez un fichier de votre ordinateur vers une clé USB, l'ordinateur lit la suite de bits correspondant au fichier sur votre disque dur en mesurant leur valeur (0 ou 1), et écrit sur la clé USB une suite de 0 et de 1 strictement identique.
On ne peut pas faire la même chose en informatique quantique, où la copie de qbits est impossible. Pourquoi ? Tout simplement parce que l'une des étapes de la copie est une mesure, et faire une mesure sur un qbit pour déterminer son état détruirait sa nature quantique (la décohérence quantique). On perd l'information contenue dans le qbit initial qui devient un bit classique, et la copie échoue : c'est le principe de non clonage.

3 - Quatre bonnes questions que vous vous posez sûrement sur l'ordinateur quantique

Physiquement, à quoi ressemble un qbit ?

Dans une clé USB, l'information est inscrite dans des semiconducteurs (des petits composants électroniques)
Dans un CD, les bits sont sous la forme de trous gravés dans un disque.

Qu'en est-il des qbits ? Comme l'information à traiter est de nature quantique, le support utilisé doit être microscopique. Jusque-là, les scientifiques ont utilisé des noyaux atomiques, des ions, des électrons ou même de simples photons.

Comment coder alors l'information sur un tel support ? Prenons l'exemple d'un l'électron qui peut avoir un spin *up* ou *down*. Notez que l'électron peut également se trouver dans un état superposé des deux états. On décide de coder le 0 avec le spin *down* et le 1 avec le spin *up*.

Et une porte quantique dans un ordi, c'est quoi ?

Une porte quantique permet de modifier l'état d'un qbit, tout comme une porte logique classique modifie l'état d'un bit. Pour modifier l'état d'un qbit, on utilise souvent des ondes électromagnétiques envoyées à une fréquence spécifique.

Pourquoi il n'y a pas encore des qbits dans nos ordinateurs ?

Sur le papier, tout se passe bien, mais il faut comprendre que l'implémentation de circuits quantiques est très délicate.

Tout d'abord, il faut que les qbits soient stables, c'est-à-dire que l'environnement les entourant ne modifie pas leur valeur par accident (par un transfert d'énergie thermique par exemple). Pour cela, les ordinateurs quantiques sont souvent refroidis à des températures très proches du zéro absolu (-273,15° !). Ainsi, les qbits sont presque totalement isolés du monde extérieur.

Faire en sorte que les qbits gardent leurs propriétés quantiques malgré leur manipulation *via* les portes quantiques est très délicat : c'est surtout sur ces problématiques que les scientifiques travaillent actuellement. Le prix Nobel de physique 2012 a été décerné aux chercheurs qui ont réussi à faire des mesures sur des objets quantiques sans les détruire, ouvrant de nouvelles possibilités pour l'informatique quantique.

Le rêve des chercheurs est de créer un ordinateur quantique universel, sur lequel on pourrait faire fonctionner n'importe quel algorithme. En attendant, certaines sociétés comme le canadien D-Wave ou Google se concentrent sur des objectifs plus précis, en fabriquant des prototypes d'ordinateurs quantiques destinés à ne résoudre qu'un seul type de problème.

Les ordinateurs quantiques vont-ils remplacer nos ordinateurs classiques ?

Les ordinateurs quantiques sont d'une telle complexité qu'ils ne sont pas destinés au grand public. Ils seraient seulement utiles pour des applications très spécifiques, là où les ordinateurs classiques sont impuissants. Pour regarder un film ou aller sur internet, les bits classiques suffisent .

La principale application pratique que l'on envisage aujourd'hui pour un ordinateur quantique est la cryptographie.

Le système de codage le plus utilisé aujourd'hui pour sécuriser la transmission de nos mails, de nos transactions bancaires, etc. est le système RSA. Le chiffrement RSA utilise des nombres premiers très grands pour sécuriser les données. Autrement dit, votre navigation est sécurisée par des calculs mathématiques très compliqués.

source : Institut Pandore