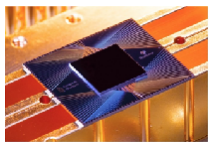
Avons-nous besoin d'un ordinateur quantique ?

Suprématie quantique

En 2019, Google a annoncé être les premiers à avoir atteint la suprématie quantique.

Cette date restera gravée dans l'histoire de l'informatique. Cet événement était attendu, mais peut-être pas aussi rapidement.

La suprématie quantique consiste à construire un processeur d'un nouveau type, un processeur quantique, puis à l'utiliser afin de réaliser un calcul qui prendrait plusieurs milliers d'années sur le plus puissant des super calculateurs existants, voire même en utilisant toutes les ressources informatiques de la planète.



Processeur Sycamore de Google composé de 53 bits quantiques et d'une surface d'1 cm².

Le plus surprenant est que le processeur construit par Google est tout petit avec une mémoire très, très réduite. Mais ce processeur peut exploiter les paradoxes de la mécanique quantique. Ce combat qui venait de commencer est celui d'un David quantique contre un Goliath supercalculateur.

Supercalculateur Summit construit par IBM, le plus au monde en 2018, occupe une surface de plus de 520 m².

Vous voulez sans doute savoir quel est ce calcul si difficile réalisé par notre David quantique. En fait ce calcul n'a été pensé que pour battre Goliath, et ne sert a priori à rien d'autre. Un calcul difficile et inutile !

2e round, 1 an plus tard. En 2020, Goliath prend sa revanche. Le calcul peut en fait être réalisé sur un simple ordinateur, comme le vôtre et le mien.

Google s'est-il trompé ? Google a-t-il exagéré ? Non, mais le combat n'était pas équitable : Goliath a été pris un peu par surprise…

La difficulté du calcul était estimée par rapport aux meilleurs algorithmes connus.

Depuis cette annonce de Google, de nombreux scientifiques ont travaillés et ont découverts de nouveaux algorithmes plus rapides. Donc match nul. Et cela en soit est aussi une prouesse mais de Goliath.

3e round, peut-être le dernier, il y a un mois : Une équipe en Chine a réussi à perfectionner le processeur quantique : le calcul reste similaire, mais encore plus difficile et plus précis. Et il semblerait bien que cette fois-ci Goliath soit KO.

Mais même s'il ne l'était pas vraiment, jamais les supercalculateurs actuels ne pourront suivre la progression des processeurs quantiques.

Pour comprendre cette compétition acharnée afin d'atteindre la suprématie quantique, par un calcul a priori inutile, nous devons revenir 40 ans en arrière.

Simulation par ordinateur

C'était l'essor de la simulation de la physique par ordinateur.

Chacun de nous peut comprendre l'intérêt de simuler certaines expériences sur ordinateur : non seulement c'est moins dangereux, moins coûteux, mais aussi potentiellement plus facile.

Essai nucléaire français en 1970 à Mururoa

Il s'agit aussi d'un grand enjeux car réaliser des expériences, ou les simuler lorsque l'on ne peut les réaliser, est indispensable à la plupart des découvertes scientifiques, que ce soit en physique, chimie ou biologie.

Mais est-ce que la simulation par ordinateur est toujours possible ?

Il s'agit en substance de la question posée par Richard Feynman lors d'une conférence en 1981. Il s'agissait en fait plutôt d'une question rhétorique car il s'empressa d'expliquer pourquoi cela était impossible concernant la simulation de la physique quantique - Impossible non seulement avec les ordinateurs de l'époque, mais aussi avec ceux d'aujourd'hui et ceux de demain, sauf peut-être si nous les pensions différemment.

Richard Feynman

Il suggéra qu'il était nécessaire de concevoir de processeurs d'un nouveau type, des processeurs quantiques - des processeurs capables de contrôler eux-mêmes des phénomènes quantiques élémentaires, afin de simuler ensuite toute la physique quantique.

Et cette fois-ci l'utilité serait donc très concrète, contrairement au calcul de Google, même s'il est impossible de dire qu'elle découverte explicite serait faîte avec ce magnifique outil, tant qu'il n'est pas construit.

Et c'est sans doute cette suggestion de Feynman qui est à l'origine de 40 années de recherche sur l'informatique quantique.

Une recherche d'abord fondamentale

Comme souvent lors d'une rupture technologique, il y a d'abord le développement d'une recherche fondamentale.

Cela a été le cas pour nos ordinateurs, grâce notamment aux travaux fondateurs d'Alan Turing.

Avant la 2e guerre mondiale, des calculateurs existaient mais ils étaient très spécialisés : on les imaginait puis on les construisait en fonction du calcul à réaliser.

Alan Turing

Avant même sa réalisation, Turing a inventé le concept d'ordinateur : c'est-à-dire un calculateur universel, sur lequel il suffirait de charger en mémoire le programme décrivant le calcul à exécuter ! Il s'agit de nos ordinateurs d'aujourd'hui que les progrès technologiques ont permis de réaliser par la suite.

Puis, c'est entre autres David Deutsch qui a repris les travaux de Turing afin de savoir s'il existait aussi un calculateur quantique universel. Non seulement il a montré que oui, mais ce dernier est au fond assez simple. Il s'agit d'un simple ordinateur qui pourrait contrôler une mémoire quantique.

David Deutsch

Le programme est donc complètement classique, et peut être écrit dès aujourd'hui.

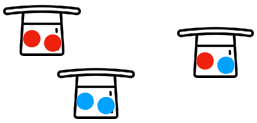
Et effectivement, de véritables environnements de programmation quantique se sont développés depuis, qui permettent de penser et coder les premiers algorithmes quantiques, qui ne demandent qu'à exécuter lorsque la mémoire quantique sera disponible.

Des algorithmes découverts sans ordinateurs !

Voyons justement ensemble un cheminement de découvertes d'algorithmes quantiques.

Deutsch a été le premier, en 1985, à concevoir un algorithme quantique. Cet algorithme ne servait qu'à démontrer la supériorité du concept d'ordinateur quantique qu'il venait de définir. Un peu comme Google, cet algorithme ne résout donc qu'un problème très artificiel.

Considérons un chapeau avec 2 boules. Soit elles sont de la même couleur, par exemple 2 rouges ou 2 bleues, soit elles sont de couleurs différentes, 1 rouge et 1 bleue.



Expérience de pensée illustrant le problème résolu par Deutsch en 1995

Combien de boules faut-il regarder pour décider si les boules sont de couleurs identiques ou non ? Facile 2.

Mais en quantique, une seule boule suffit. Un peu comme le chat de Schrödinger qui serait à la fois mort et vivant, un ordinateur quantique peut sans réellement choisir quelle boule il observe, arriver à décider si elles sont de couleurs identiques. Cela semble magique, mais pourtant bien réalisable dans le monde quantique.

Cela semble aussi assez futile. Et pourtant, 9 ans plus tard, ces idées ont permis de découvrir l'analogue quantique de la bombe de Turing. C'est-à-dire un algorithme quantique qui mettrait à mal la plupart de notre sécurité informatique, que ce soit sur internet, sur nos téléphones ou encore sur notre CB. Mais ne vous inquiétez pas pour votre CB, l'ordinateur quantique n'existe pas encore, et donc l'algorithme ne peut pas être utilisé.

Très rapidement les mêmes idées de cet algorithme terrifiant ont permis de répondre à la question de Feynman : OUI un ordinateur quantique permettrait de simuler efficacement toute la physique quantique.

13 ans plus tard, cette simulation quantique permettrait à son tour de résoudre un problème bien mathématique, sur lequel vous avez sans doute tous sué au lycée, à savoir la résolution de systèmes linéaires.

$$\begin{cases} 2x + 3y - z = 5 \\ x - y + 7z = 20 \\ -x + 2y + 3z = 12 \end{cases}$$

Système linéaire à 3 équations et 3 inconnues

Ces systèmes sont partout, notamment en intelligence artificielle, et c'est donc très naturellement que l'intelligence artificielle quantique s'est développée ensuite.

Lorsqu'on voit les progrès faits depuis le problème de Deutsch avec les boules rouges et bleues, on se dit que finalement il y a de l'espoir avec le calcul a priori inutile réalisé par Google.

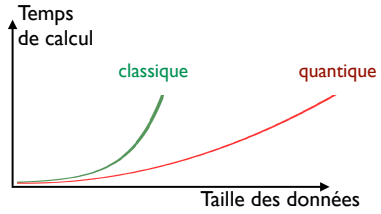
Quelle accélération ?

Mais de quelle accélération quantique parle-t-on au juste ?

Tout d'abord, tout n'a pas besoin d'être accéléré. Inutile d'avoir un ordinateur quantique pour faire tourner Word, Excel ou autre.

Mais plus surprenant, il y a des calculs pour lesquels les ordinateurs quantiques ne seront jamais plus rapides : que ce soit pour une simple addition, trier des données, ou encore démontrer un théorème mathématique.

Mais pour beaucoup de problèmes l'accélération est asymptotique. L'ordinateur quantique n'est pas 2 fois, 10 fois ou 100 fois plus rapide : son accélération est d'autant plus grande que le problème manipule de grandes données, et donc d'autant plus que la taille de la mémoire quantique est grande.

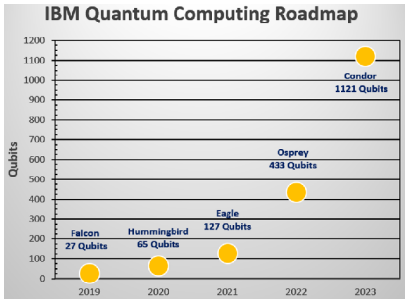


Accélération asymptotique : l'accélération augmente avec la taille des données

Hélas, les processeurs quantiques actuels sont encore trop petits, que ce soient ceux de Google, de Chine, ou ici d'IBM.

Leur mémoire de 50 à 100 bits quantiques permet à peine de stocker un numéro de téléphone. Les prochains stockeront quelques phrases.

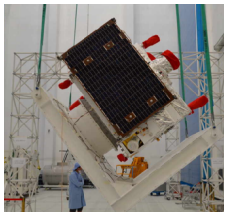
Alors, est-ce que ce sera suffisant ? Peut-être !



Evolution des processeurs quantiques d'IBM

Quels usages en attendant ?

Avec un seul bit quantique, il est possible de chiffrer toute communication avec une sécurité qui repose sur les lois de la physique quantique. Certes il ne s'agit pas de calcul, mais la technologie est prête. La Chine a même envoyé un satellite pour l'expérimenter dans l'espace.



Satellite envoyé en 2016 par la Chine pour déployer dans l'espace la communication quantique

Avec quelques bits quantiques de plus, il est possible de déployer un internet quantique.

Aujourd'hui, nous sommes probablement entrés dans l'ère de la suprématie quantique. Mais il s'agit maintenant de faire travailler ensemble David et Goliath. En associant les super calculateurs actuels à des processeurs quantiques, nous espérons faire de nouveaux calculs à la fois utiles et impossibles auparavant.

Une des premières applications pourrait bien être la simulation quantique comme l'avait suggérée Feynman il y a 40 ans !

Bien entendu, dans un futur idéal, nous aurons des mémoires de millions à milliards de bits quantiques. Au fond, ce n'est rien de plus qu'une grosse clé USB - quantique. Nous aurions alors accès à un ordinateur quantique complet.

Certes, une partie de notre sécurité informatique serait compromise, mais nous avons déjà plusieurs parades en préparation, dont justement une quantique.

Mais surtout nous pourrions tirer profit des nombreux algorithmes quantiques déjà découverts et qui n'attendent qu'à être utilisés sur un ordinateur quantique.

Enjeux stratégiques

En conclusion, l'ordinateur quantique est source de spéculations et fantasmes.

Les enjeux sont grands. L'avantage que cette machine procurerait à une entreprise ou une nation est incommensurable.

Sans attendre, il nous faut œuvrer collectivement pour ne pas se faire distancer, et au contraire être à la table de ceux qui maîtrisent cette technologie, et surtout de faire en sorte que les retombées profitent au plus grand nombre.

Le pouvons-nous ? En France ? Plusieurs des pionniers de cette recherche sont en France, en particulier au CNRS où je travaille, et plus largement en Europe. Plusieurs de nos start-ups possèdent actuellement une technologie qui fait concurrence à celle des plus grands groupes internationaux. Plusieurs de nos industries se sont déjà engagées dans cette aventure. Donc oui, nous le pouvons.

Et si cela ne marchait pas ? Si aucun ordinateur quantique ne venait à voir le jour ?

Il ne faut pas s'en inquiéter. A chaque fois, dans l'histoire scientifique, qu'un tel effort technologique a été motivé par une recherche fondamentale, de qualité et collective, de grandes découvertes ont été faites, mais parfois pas là où on les attendait.

Qui aurait pensé que le laser allait permettre de développer internet et de soigner des gens ?

Donc, bien malin celui qui peut prévoir si un ordinateur quantique existera un jour ou non. Mais les efforts faits pour sa réalisation auront des répercutions sans précédent. Faisons simplement en sorte d'être acteur dans cette révolution.

Epilogue : solution au problème du chapeau

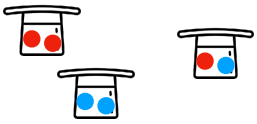
L'expérience de pensée du chat de Schrödinger met en évidence les paradoxes de la physique quantique lorsqu'ils sont interprétés dans notre monde réel. Néanmoins, à l'échelle des particules élémentaires, l'état d'un système binaire, 0 ou 1, est effectivement non déterminé avant son observation. Il est en *superposition*, un peu comme une pièce 0/1 qui tournerait en permanence tant qu'elle n'est pas saisie pour être observée. La réalité quantique autorise en plus ces probabilités à être négatives ! Elles permettent des phénomènes bien étranges tels que des interférences destructives.

Ces probabilités négatives, appelées *amplitudes*, apparaissent naturellement dans l'étude des ondes. Une onde (comme une vague) peut avoir une amplitude positive (au-dessus du niveau de la mer) ou négative (en-dessous du niveau de la mer). Elles permettent d'expliquer le comportement de deux ondes s'entrechoquant à la surface de l'eau, ou en optique avec l'expérience des fentes de Young[1]. Ces interférences sont utilisées pour annuler les bruits extérieurs dans certains casques auditifs. A l'échelle des particules, l'état d'une particule peut "osciller" entre plusieurs configurations avec des amplitudes positives ou négatives.

Ces amplitudes permettent en théorie d'inverser le lancé d'une pièce 0/1. Un peu comme une fonction de visionnage arrière. Comment est-ce possible ? Tout simplement, le signe des amplitudes est utilisé pour coder la face de la pièce avant le lancé. La physique quantique nous dit qu'il est alors possible de revenir en arrière.

Ainsi si on part de la face 0, les amplitudes après le lancé sont de même signe. En revanche si on part de la face 1, les amplitudes après le lancé seront de signes opposés. La valeur de l'amplitude, sans son signe, est liée à la probabilité de retomber du côté 0 ou 1. Au signe près, elle est donc la même dans tous les cas.

Retournons à notre chapeau contenant 2 boules rouges ou bleues. Comment savoir si elles sont de la même couleur en en regardant qu'une seule ? Voici la stratégie, ou algorithme, imaginée par Deutsch :



- Choisir au hasard une boule à l'aide d'un lancé quantique d'une pièce 0/1 initialement du côté 0 : Si le côté est 0, prendre la boule de gauche, sinon la boule de droite.
- Si la boule est rouge, changer le signe de l'amplitude de la pièce
- Inverser le lancer de pièce
- Si la pièce est du côté 0, déclarer que les boules sont de la même couleur, sinon de couleurs différentes

Analysons maintenant l'algorithme :

- Si les 2 boules sont bleues, aucune amplitude n'est modifiée. L'inversion du lancer nous ramène donc au côté 0.

- Si une des boules est rouge, et l'autre bleue, alors les amplitudes sont de signes différents après la deuxième étape, comme si le lancé avait été effectué depuis le côté 1. L'inversion du lancé nous amène donc au côté 1.

[1] Cette vidéo illustre très bien le phénomène : https://youtu.be/Iuv6hY6zsd0

- Enfin, si les 2 boules sont rouges, les amplitudes deviennent toutes deux negatives après la deuxième étape, mais de même signe ! L'inversion du lancer nous ramène au côté 0.

Nous avons donc résolu le problème en n'utilisant qu'une seule boule, mais en superposition… La difficulté à réaliser cet algorithme est donc de l'exécuter dans une réalité quantique. Dans ce cas précis, il s'agit d'une expérience d'interférométrie très utilisée de nos jours en optique. Le défis des prochains calculateurs quantiques sera de programmer des algorithmes quantiques qui manipulent plusieurs milliers de pièces et boules en superposition quantique.