L'informatique quantique

Table des matières :

Introduction :

The concept of quantum computing was born in the 1980s after scientists began to consider using quantum mechanical properties to solve difficult calculations.

While conventional computers manipulate conventional binary values of 0 or 1 to perform calculations, quantum computers use so-called qubits, which are capable of representing an exponential number of values compared to bits. These qubits interact in such a way that they can perform certain computational tasks much faster than a conventional computer.

Quantum computing - a new revolution in the industrial world?

First, we will see why quantum computing is of global interest. Then we will look at the technical obstacles to be overcome.

I- A global interest

Although no quantum computer is yet sophisticated enough to perform these calculations, governments, technology giants and investors are already preparing for this revolution in the making. It's a quantum computer race, driven largely by the technological upheaval the machine is expected to bring. And for good reason: the nation that takes the lead in quantum computing is expected to play a leading role in the future. Several nations have jumped into the quantum computing industry, including the US and China. Google, which claims to have succeeded in creating a processor capable of performing a calculation in 200 seconds when the most advanced computer today would take 10,000 years.

A revolution expected in many areas

It is this ability to take a gigantic number of paths that makes quantum computers much faster than conventional computers. Quantum computers will not replace current systems, but will be used for different types of problems, incredibly complex ones, where eliminating a wide range of possibilities will save a lot of time.

An example often cited is the execution of certain algorithms, much faster, which could notably make it possible to factor in prime numbers, to solve the traveller's problem (path optimisation), to search in databases, or to simulate complex differential equations.

A quantum computer could also make it possible to invent molecules, simulate new materials, solve problems related to logistics or even accurately simulate chemical reactions that still seem mysterious to us.

II- Technical obstacles to be solved

But before the potential of the quantum computer can be realised, many barriers still need to be removed before it can become a reality.

Decoherence is the major obstacle: the quantum computer, in order to calculate much faster and more efficiently than a classical computer, will use the superposition and entanglement of states which are much more sensitive to the environment than classical states. The more qubits are added to a system, the more the number of parallel operations will be increased and, consequently, the computing power as well. It is estimated that nearly 300 qubits perfectly entangled in superposition could map all the information in the universe from the Big Bang.

However, when the environment interacts with the qubits (which is necessary for the quantum measurement to work), it will uncontrollably change their quantum states. This is called decoherence. Decoherence can arise from many aspects of the environment: changes in magnetic and electric fields, radiation from nearby hot objects or uncontrolled interactions between qubits.

Decoherence affects the superposition state and disrupts quantum information processing. This leads to errors in quantum computing systems. While a classical computer is very reliable, a quantum computer would make one error in 1,000 operations (for the best of them).

Challenges for the future

So how do we break down these barriers? To see a quantum computer succeed in executing viable calculations and thus revolutionise a number of fields, it would be necessary to manufacture, control and measure several qubits, create quantum gates and finally develop algorithms that would take advantage of quantum acceleration.

There is a limit to how long qubits can retain their quantum properties before errors disrupt the computational mechanism. This is called the coherence length. In order to reduce the risk of errors in the calculations carried out by a quantum computer, it would therefore be necessary to have qubits with a coherence length long enough to calculate mathematical problems.

And to increase this coherence length, researchers are now working on developing error reduction algorithms using a quantum error correction code (the first of which was developed by Peter Shor). This allows them to encode a logical qubit into several physical qubits, so that errors become tractable. It should also be possible to perform logic gates, in order to improve the performance of operations.

In any case, it would take hundreds of millions of coherently connected qubits to have a universal quantum computer. The few quantum machines that exist today cannot, for the moment, handle as many qubits as would be needed to scale up. "Given the information available, it is still too early to predict when a quantum computer of sufficient size will exist,"

explained The National Academies of Sciences, Engineering, and Medicine in 2019, in a report entitled Quantum Computing: Progress and Prospects.

In the meantime, in France, the quantum ecosystem is tending to become structured: scientists, industrialists, start-ups and political decision-makers have already launched themselves into the race for quantum acceleration, working in particular on the deployment of quantum infrastructures, but also on what will make it possible to exploit and develop the possibilities offered by the hardware architectures.

Conclusion :

Nous pouvons donc dire que l'informatique quantique représente une nouvelle révolution dans le monde industrielle. En effet, l'ordinateur quantique d'ici quelque année devrait enfin atteindre la suprématie quantique et devrait ainsi avoir le potentiel de résoudre certains types de problèmes, aujourd'hui insolubles.

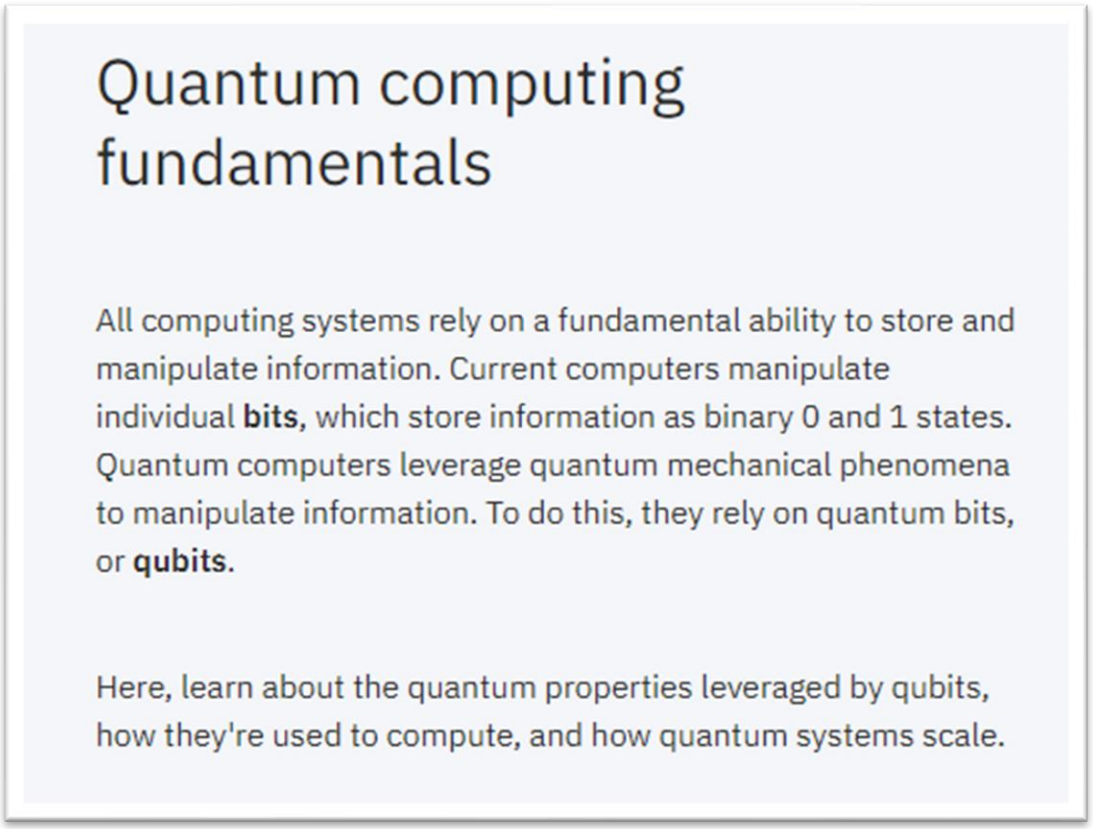
Parmi ceux-ci, citons par exemple la simulation de l'enzyme nitrogénase, qui permettrait de contourner le procédé Haber-Bosch (ce procédé, optimisé pour son époque - tout début du XXe siècle - conduit pourtant à consommer 3 à 5 % de l'ensemble du gaz naturel produit, et environ 1 à 2 % des réserves mondiales en énergie, pour la synthèse de l'ammoniac). Un ordinateur quantique pourrait ainsi permettre de comprendre comment cette enzyme fonctionne, pour pouvoir catalyser à température ambiante et fabriquer des engrais azotés, sans chauffer.

Mais l'informatique quantique est une matière délicate car il est difficile de stabiliser les qubits dans leur état quantique. Cela nécessite des conditions très précises : des atomes simples, froids, isolés du monde extérieur. Et les difficultés augmentent à mesure que leur nombre croît. Si bien que les fabricants peinent aujourd'hui à dépasser les 53 qubits.

Saluée par la Maison Blanche, réjouie de devancer la Chine, la performance de Google a cependant été relativisée par IBM qui affirme qu'elle aurait pu être réalisée en trois jours avec le plus puissant des ordinateurs classiques dont la puissance de calcul aurait été affectée à cette unique tâche. Plusieurs experts ont aussi appelé à la prudence, soulignant que ce calcul spécifique n'était pas utile et que le chemin était encore long avant l'avènement d'un ordinateur quantique universel.

Bibliographie :

Article 1 :



Résumé :

Les systèmes informatiques, ont une capacité de stockage et de manipulation des informations. Les ordinateurs d'aujourd'hui fonctionne en utilisant les bits, en stockant les informations en binaire donc en manipulant les 0 et les 1. L'informatique quantiques est totalement différente. En effet, cette technologie utilise les phénomènes de la mécanique quantique pour gérer les informations. L'informatique quantiques ne manipulent pas de bits individuels mais des bits quantiques, appelé qubits.

Article 2 :

Ce que peut l'informatique quantique

Si vous avez déjà programmé une macro Excel, alors vous avez certainement vécu ce qui suit : vous ajoutez des lignes de saisie au bas d'une feuille de calcul dont les colonnes servent d'entrées pour une formule longue. Chaque fois que la formule se recalcule, le temps de calcul se fait de plus en plus long. Si vous travaillez sur un ordinateur assez lent, vous pouvez être témoin de ce phénomène par vous-même : comme le nombre de lignes d'entrée augmente linéairement, le temps consommé par la macro croît de façon exponentielle.

Maintenant, si vous faites partie des chanceux à avoir déjà écrit un programme pour un superordinateur, vous avez pu être également témoin du même phénomène. L'échelle peut être différente, mais l'effet est le même. Et si vous lisez les journaux de log du superordinateur, vous pouvez vérifier personnellement cette observation. Pour résumer : il vient un moment où chaque algorithme, aussi simple soit-il, devient tout simplement inapplicable en raison du poids écrasant de ses données d'entrée.

C'est là que l'informatique quantique entre en jeu. En supprimant purement et simplement ce phénomène d'allongement des durées de calcul. En théorie, un ordinateur quantique pleinement fonctionnel deviendra en effet plus performant de façon exponentielle. Comment ? Tout simplement en mettant à l'échelle sa capacité de calcul de façon linéaire. Par conséquent, pour chaque augmentation du nombre d'étapes d'un algorithme quantique, la quantité de temps consommée pendant l'exécution des calculs augmentera d'une plus petite quantité, jusqu'à ce que l'écart de temps entre des charges de travail exponentiellement différentes devienne si infime qu'il ne pourra plus être mesuré.

Résumé :

L’informatique quantique permet d’exécuter des algorithmes, des programmes ou encore des calcules beaucoup plus rapidement que les ordinateurs grands publique. En effet, par exemple sur Excel lorsqu’on ajoute des lignes de saisie au bas d'une feuille de calcul dont les colonnes servent d'entrées pour une formule longue. Chaque fois que la formule se recalcule, le temps de calcul se fait de plus en plus long et l’ordinateur devient moins performant.

L’informatique quantique résout se problème très facilement. En effet, cette technologie supprime le phénomène d’allongement des durées de calcul et devient plus puissant de manière exponentielle. Pour cela, l’informatique quantique met à l’échelle sa capacité de calcul de façon linéaire.

Article 3 :

- **Chiffrement :** pour certains, il s'agit là d'une réelle opportunité. Un concept appelé distribution de clés quantiques (QKD - quantum key distribution) permet d'espérer théoriquement que les clés publiques et privées que nous utilisons aujourd'hui pour chiffrer les communications pourront bientôt être remplacées par des clés quantiques soumises aux effets de l'intrication.
  Théoriquement, toute tierce partie brisant la clé et tentant de lire le message détruirait immédiatement le message pour tout le monde. La théorie de la QKD est basée sur une hypothèse énorme qui doit encore être testée dans le monde réel : que les valeurs produites avec des qubits enchevêtrés sont elles-mêmes enchevêtrées et sujettes à des effets quantiques partout où elles vont.

Résumé :

L'informatique quantique, propose une plus grande sécurité au niveau du chiffrement d'information par rapport à l'informatique actuelle. En effet, les clés de chiffrement seront beaucoup plus sécurisées par des clés quantiques soumises aux effets de l'intrication. En mécanique quantique, l'intrication quantique, ou enchevêtrement quantique, est un phénomène dans lequel deux particules (ou groupes de particules) forment un système lié, et présentent des états quantiques dépendant l'un de l'autre quelle que soit la distance qui les sépare. De même, lorsqu'une personne brise la clé quantique et tante de lire le message, ce dernier se détruirait immédiatement pour tout le monde.

Article 4 :

Quantum computers are great for solving optimisation problems from figuring out the best way to schedule flights at an airport to determining the best delivery routes for the FedEx truck.

Google announced it has a quantum computer that is 100 million times faster than any classical computer in its lab.

Every day, we produce 2.5 exabytes of data. That number is equivalent to the content on 5 million laptops. Quantum computers will make it possible to process the amount of data we're generating in the age of big data.

In order to keep quantum computers stable, they need to be cold. That's why the inside of D-Wave Systems' quantum computer is -460 degrees Fahrenheit.

According to Professor Catherine McGeoch at Amherst University, a quantum computer is "thousands of times" faster than a conventional computer.

Superposition is the term used to describe the quantum state where particles can exist in multiple states at the same time, and which allows quantum computers to look at many different variables at the same time.

Rather than use more electricity, quantum computers will reduce power consumption anywhere from 100 up to 1000 times because quantum computers use quantum tunnelling.

Quantum computers are very fragile. Any kind of vibration impacts the atoms and causes decoherence.

Résumé :

Les ordinateurs quantiques sont parfaits pour résoudre optimisation des problèmes de détermination de la meilleure façon de planifier les vols dans un aéroport à la détermination des meilleurs itinéraires de livraison pour le camion FedEx.

Google a annoncé avoir un ordinateur quantique 100 millions de fois plus rapide que n'importe quel ordinateur classique de son laboratoire.

Afin de maintenir la stabilité des ordinateurs quantiques, ils doivent être froids. C'est pourquoi l'intérieur de l'ordinateur quantique de D-Wave Systems est à -460 degrés Fahrenheit.

Selon le professeur Catherine McGeoch de l'Université d'Amherst, un ordinateur quantique est « des milliers de fois » plus rapide qu'un ordinateur conventionnel.

Plutôt que d'utiliser plus d'électricité, les ordinateurs quantiques réduiront la consommation d'énergie de 100 à 1000 fois parce que les ordinateurs quantiques utilisent le tunnelling quantique.

Les ordinateurs quantiques sont très fragiles. Tout type de vibration a un impact sur les atomes et provoque une décohérence.

Article 5 :

Lingua quantum

From there, dedicated software frameworks and programming languages allow researchers to simulate, execute and explore the quantum circuits they design. Several of these languages were described in a 2020 review (B. Heim *et al. Nature Rev. Phys.* **2**, 709–722; 2020).

Microsoft, IBM and Google have all created tools – Q#, Qiskit and Cirq, respectively – that draw heavily on the Python programming language, and have built user-friendly development environments with ample documentation to help coders get started. Microsoft, for example, has created a full quantum development kit (QDK), containing code libraries, a debugger and a resource estimator, which checks in advance how many qubits an algorithm will require.

And it's not just the technology giants that are involved. Rigetti Computing in Berkeley, California, which has its own 31-qubit machine, has released a quantum-software development kit called Forest, which includes a Python library called pyQuil. And UK-based Cambridge Quantum Computing has launched tket, with the associated pytket library.

Résumé :

De grand acteurs du monde informatique, comme Microsoft, IBM et Google ont déjà leur propre ordinateur quantitque et on déjà créer des outils de programmations pour concevoir cette technologie afin de l'ameliorer. En effet, on retrouve different langages comme Q#, Qiskit et Cirq. De même, Microsoft, par exemple, a créé un kit de développement quantique complet (QDK), contenant des bibliothèques de code, un débogueur et un estimateur de ressources, qui vérifie à l'avance le nombre de qubits requis par un algorithme. Rigetti Computing a egalemnt publiée une bibliothèque Python appelée pyQuil.

Article 6 :

Once a stable quantum computer gets developed, expect that machine learning will exponentially accelerate even reducing the time to solve a problem from hundreds of thousands of years to seconds.

Remember when IBM's computer Deep Blue defeated chess champion, Garry Kasparov in 1997? It was able to gain a competitive advantage because it examined 200 million possible moves each second. A quantum machine would be able to calculate 1 trillion moves per second!

This year, Google stated publicly that it would produce a viable quantum computer in the next 5 years and added that they would reach "quantum supremacy" with a 50-qubit quantum computer. The top supercomputers can still manage everything a five- to 20-qubit quantum computer can, but will be surpassed by a machine with 50 qubits and will attain supremacy at that point. Shortly after that announcement, IBM said it would offer commercial quantum machines to businesses within a year.

Even though a true quantum computer is still not a reality, it's clear that the race is on.

Résumé :

Lorsqu'un ordinateur quantique stable sera terminé, l'apprentissage automatique s'accéléra de manière exponentielle, même en réduisant le temps de résolution d'un problème de centaines de milliers d'années à quelques secondes. De même, un ordinateur grand publique est capable de calculer 200 millions de coups possibles lors d'une partit d'échecs. Un ordinateur quantique quant à lui sera capable de calculer 1 billion de mouvements possibles par secondes.

Cette année, Google a déclaré publiquement qu'il produirait un ordinateur quantique viable dans les 5 prochaines ans et a ajouté qu'ils atteindraient la « suprématie quantique » avec un ordinateur quantique de 50 qubits. Peu de temps après cette annonce, IBM a déclaré qu'il proposerait des machines quantiques commerciales aux entreprises d'ici un an.

Article 7 :

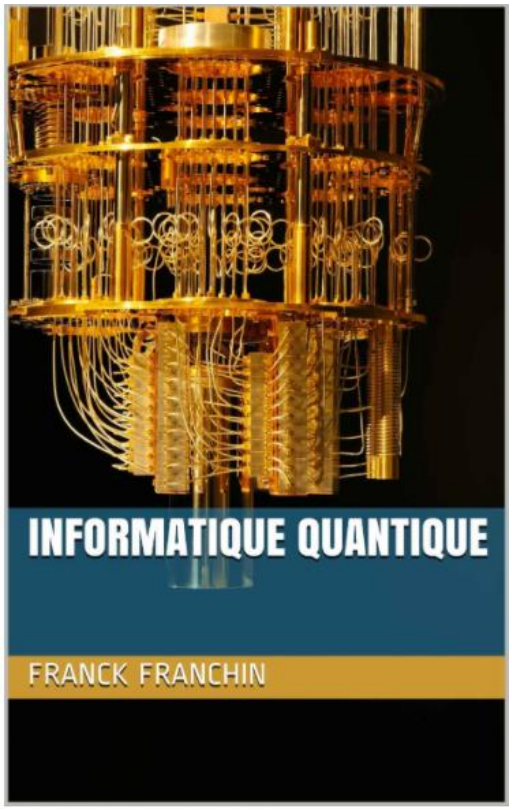
Vidéo Youtube : What is Quantum Computing? Easy Explanation With Practical Examples

https://www.youtube.com/watch?v=6T2np_Q-dYE

Article 8 :

Livre : Informatique Quantique: Collection « 60 min pour comprendre ».

De Franck FRANCHIN (Auteur), Alessandro Curioni (Préface), Charles Beigbeder (Préface)



Sources :

https://www.zdnet.fr/pratique/tout-comprendre-a-l-informatique-quantique-39891035.htm

https://www.lefigaro.fr/secteur/high-tech/au-fait-c-est-quoi-l-informatique-quantique-20210121

https://www.futura-sciences.com/sciences/definitions/physique-ordinateur-quantique-4348/

https://www.lebigdata.fr/informatique-quantique-big-data

https://www.inria.fr/fr/comment-fonctionne-un-ordinateur-quantique

https://www.01net.com/actualites/l-informatique-quantique-des-promesses-incroyables-mais-difficiles-a-tenir-2035451.html

https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/

https://mitpress.mit.edu/books/quantum-computing

https://www.bernardmarr.com/default.asp?contentID=1193#:~:text=Classical%20computers%20manipulate%20ones%20and,zero%20at%20the%20same%20time.

https://www.nature.com/articles/d41586-021-00533-x