

Comment l'informatique quantique pourrait révolutionner notre monde

Plaque de qbits physiques réalisés par Intel (technologie basée sur la supraconductivité) - GK/01net.com

Calcul de molécules complexes, intelligence artificielle, problèmes d'optimisation... Les bénéfices de l'informatique quantique sont potentiellement énormes dans un grand nombre de domaines.

Google, IBM, Intel, Microsoft... Depuis plusieurs mois, les géants de l'informatique multiplient les annonces pour montrer les efforts qu'ils entreprennent dans l'informatique quantique. Ce domaine de recherche est actuellement l'un des plus dynamiques dans le domaine high-tech. Les coopérations et partenariats fusent de tous les côtés. Les industries classiques sont également parties prenantes, car elles espèrent que l'informatique quantique leur permettra de franchir un nouveau de cap dans leur innovation. Parmi les partenaires du programme de recherche quantique d'IBM figurent, par exemple, des banques (JP Morgan Chase, Barclays), des constructeurs automobiles (Daimler, Honda), des fabricants de produits chimiques et de matériaux (Nagase, Hitachi Metals, JSR Corporation).

Pour comprendre cet engouement général, il faut rappeler quelques principes du calcul quantique. Celui-ci s'appuie sur l'utilisation de « bits quantiques » ou qbits qui ont la particularité de valoir à la fois 0 et 1. Cette propriété découle directement du principe de superposition quantique qui fait qu'une particule peut avoir plusieurs valeurs d'état en même temps. Un exemple d'état est le spin, qui décrit le sens de rotation d'une particule.

Un parallélisme massif et naturel

L'avantage au niveau informatique, c'est que cette superposition confère à un ordinateur quantique une puissance de calcul naturellement exponentielle. Un registre de N qbits peut avoir en même temps 2^N valeurs que l'on pourra transformer avec une succession de portes logiques quantiques. Toutes ces opérations s'appliqueront simultanément sur les 2^N valeurs, de sorte que l'on aura à la fin une superposition de 2^N résultats.

« D'une certaine façon, la mécanique quantique fournit gratuitement du parallélisme massif. Mais ce parallélisme est un peu fictif, car lorsqu'on effectue une lecture du registre, la superposition quantique s'évanouit et on n'obtient qu'un des états de base. Tout l'art de l'algorithmique quantique est donc de faire en sorte qu'à la fin de calculs, on obtient un résultat intéressant », explique Daniel Estève, directeur de recherche et chef du groupe Quantronique dans le service de physique de l'état condensé au CEA.

Ce potentiel de puissance de calcul fait entrevoir tout un tas d'applications concrètes, à commencer par... l'espionnage. Contrairement aux ordinateurs classiques, un ordinateur quantique a théoriquement la capacité de factoriser assez rapidement les grands nombres en nombres premiers. Ce qui signifierait la mort de la cryptographie à clé publique, <https://www.01net.com/actualites/pourquoi-l-informatique-quantique-pourrait-aneantir-le-web-tel-que-nous-le-connaissons-650502.html>

une technologie qui est aujourd'hui à la base de tous les échanges numériques. Il n'est donc pas étonnant que la NSA dispose, elle aussi, d'un programme de recherche quantique.

Trouver les molécules par un calcul exact

Mais il y a aussi des manières plus constructives d'envisager l'informatique quantique. L'un des premiers secteurs qui devraient en profiter est la chimie et la physique des matériaux.

Un ordinateur quantique devrait permettre de trouver beaucoup plus rapidement de nouvelles molécules aux propriétés intéressantes. Actuellement, il est très difficile de simuler les propriétés

des molécules de manière informatique. Le calcul s'appuie sur l'équation dite de Schrödinger qui est particulièrement complexe et qui est hors de portée des calculateurs classiques.

« Plus il y a d'atomes, plus il y a d'interactions entre ces atomes, et cette complexité augmente de manière exponentielle. Au niveau d'une simulation, on est donc rapidement limité dans la taille des agrégats moléculaires », nous expliquent Christophe Calvin, responsable du secteur informatique, simulation numérique et calcul intensif au CEA/DRF, et Christian Gamrat, responsable scientifique du département architecture conception et logiciels embarqués au CEA/List. Les deux hommes ont d'ailleurs cosigné un article sur ce sujet dans le dernier numéro de « Clefs » <http://www.cea.fr/multimedia/Pages/editions/clefs-cea/revolutions-quantiques.aspx>, une revue éditée par le CEA.

Pour arriver à leurs fins, les chercheurs sont donc obligés d'appliquer des ensembles d'approximations qui nécessitent beaucoup d'expérimentations pour obtenir un résultat correct à la fin. La puissance de calcul d'un ordinateur quantique permettrait, de son côté, de réaliser un calcul exact sans approximations, d'où un gain de temps considérable.

Selon Microsoft, un ordinateur quantique avec 100-200 qubits permettrait, par exemple, de concevoir un catalyseur pour extraire le dioxyde de carbone de l'atmosphère et, peut-être, de résoudre le problème du réchauffement climatique.

On peut également imaginer trouver de nouveaux matériaux supraconducteurs à température ambiante, ce qui permettrait une transmission de courant sans perte. Une réponse définitive au défi des composants électroniques actuels ? Les répercussions au niveau de notre quotidien seraient énormes.

Réduire les itérations dans l'optimisation

L'autre grand domaine d'application envisagé du calcul quantique est l'optimisation, c'est-à-dire le fait de trouver le minimum ou le maximum d'une fonction. Cette catégorie de problème existe dans de nombreux domaines différents : gestion de trafic, calcul d'itinéraire, emplois du temps, problèmes d'ordonnancement et de planification, calcul d'un risque financier, etc.

Ces problèmes, très concrets, peuvent rapidement devenir très complexes, si le nombre de variables est trop important. Un cas particulier de l'optimisation est l'apprentissage automatique qui consiste généralement à minimiser une fonction d'erreur.

Tous ces procédés sont actuellement très itératifs et approximatifs. L'apprentissage automatique, par exemple, s'appuie souvent sur la lecture de plusieurs millions voire dizaines de millions d'objets à analyser. La superposition de valeurs de l'informatique quantique pourrait alors se révéler intéressante.

Mais il est probable que la résolution des problèmes d'optimisation ne viendra que dans un second temps, après le calcul de molécules. Ce dernier pourra s'appuyer sur des bibliothèques d'atomes artificiels pour être réalisé. Les problèmes d'optimisation, au contraire, partent d'une situation où les contraintes sont différentes à chaque fois. Ils nécessitent donc un travail de préparation et d'initialisation beaucoup plus lourd. Chaque domaine doit trouver ce que peut apporter l'informatique quantique aux problèmes auxquels il se confronte. Pour y arriver ces différents secteurs doivent aborder des voies technologiques différentes... Nous les explorerons dans un prochain article.

<https://www.01net.com/actualites/comment-l-informatique-quantique-pourrait-revolutionner-notre-monde-1475739.html>