ACTUALITÉS

INFORMATIQUE

L'AVANTAGE QUANTIQUE ATTEINT AVEC DES PHOTONS

Ce dispositif photonique a permis de calculer en 200 secondes une grandeur dont le calcul sur un supercalculateur actuel aurait pris 2,5 milliards d'années.

Un dispositif photonique a surclassé en vitesse de calcul les meilleurs supercalculateurs actuels. Une prouesse de plus vers l'avènement des ordinateurs quantiques.

En 2019, Google a fait une annonce fracassante : ses équipes ont affirmé avoir atteint l'« avantage quantique » (aussi nommé « suprématie quantique »). Cette expression correspond au stade où un ordinateur quantique, dispositif encore largement en devenir, est capable d'effectuer un certain calcul beaucoup plus vite que n'importe quel ordinateur « classique ». Le résultat de Google a été rapidement contesté et a alimenté une farouche compétition autour de la réalisation de l'avantage quantique. Aujourd'hui, c'est une équipe chinoise menée par Jian-Wei Pan et Chao-Yang Lu, de l'université des sciences et des technologies de Hefei, qui affirme avoir atteint ce stade, par une tout autre approche que celle de Google.

Un ordinateur classique manipule l'information sous la forme de bits, qui prennent la valeur « 0 » ou « 1 ». L'ordinateur quantique, lui, manipule des bits quantiques, ou qubits, qui reposent sur le principe quantique de superposition des états : un qubit peut être une superposition de l'état « 0 » et de l'état « 1 ». Cette subtilité, si elle est correctement exploitée, permet en théorie de réaliser certains calculs beaucoup plus vite qu'avec des dispositifs classiques.

Une analogie courante est celle de l'exploration d'un labyrinthe : là où un ordinateur classique ne peut suivre qu'un chemin à la fois, un ordinateur quantique les explore tous simultanément, gagnant ainsi beaucoup de temps. Autre exemple plus concret : l'implémentation de l'algorithme quantique de Shor (conçu par Peter Shor) permettrait de calculer très vite la décomposition en facteurs premiers d'un entier très grand. Or de nombreux systèmes cryptographiques reposent aujourd'hui sur le fait qu'un ordinateur classique met un temps rédhibitoire pour exécuter une telle tâche.

Construire un ordinateur quantique est cependant un véritable défi technologique. Un état de superposition quantique est très fragile et la moindre perturbation due à l'environnement réduit à néant les performances du dispositif. D'où la difficulté à fabriquer de telles machines, et de nombreuses approches sont à l'étude pour réaliser des qubits.

Par exemple, le processeur quantique Sycamore de Google utilise des circuits supraconducteurs. Avec 53 qubits, il a réalisé en 200 secondes un calcul « inutile », mais conçu spécifiquement pour être difficile à traiter sur une architecture classique. L'équipe de Google a affirmé qu'il faudrait 10000 ans sur un supercalculateur pour arriver au même résultat. Mais peu de temps après, IBM a annoncé être capable d'effectuer

ce même calcul en seulement deux jours et demi grâce à une optimisation de l'algorithme classique. Sycamore est certes plus rapide, mais l'écart n'est pas si grand. Peut-on alors vraiment parler d'avantage quantique ?

La course est relancée avec le dernier résultat de l'équipe de Jian-Wei Pan et Chao-Yang Lu. L'approche de ces chercheurs s'appuie sur l'échantillonnage de bosons, une idée proposée en 2011 par Scott Aaronson, aujourd'hui à l'université du Texas à Austin, et Alex Arkhipov, son doctorant à l'époque. Cette méthode est aussi conçue spécifiquement pour atteindre l'avantage quantique avec un calcul inutile, mais très difficile à reproduire sur un ordinateur classique. Le principe revient à envoyer en parallèle un certain nombre de photons (qui font partie de la famille des bosons) individuels et indiscernables dans un système optique constitué d'un réseau de miroirs semi-réfléchissants. Les sorties du dispositif sont équipées de détecteurs de photons uniques.

Le système agit comme un interféromètre de grande taille et on cherche à calculer les probabilités jointes de détection de photons, c'est-à-dire les corrélations entre plusieurs détecteurs (par exemple la probabilité d'avoir un signal sur les détecteurs 3, 8 et 14 ; ou sur les détecteurs 1, 2, 3 et 7 ; etc.). Un ordinateur classique calcule avec difficulté ces probabilités. Pour les obtenir, le calcul complet prend la forme d'une matrice dont il faut estimer le « permanent », une grandeur qui se rapproche du déterminant de la matrice, mais qui est bien plus fastidieuse à calculer. La complexité de ce calcul croît exponentiellement avec le nombre de photons détectés. Au-delà de quelques dizaines de photons, le résultat est hors de portée des ordinateurs classiques.

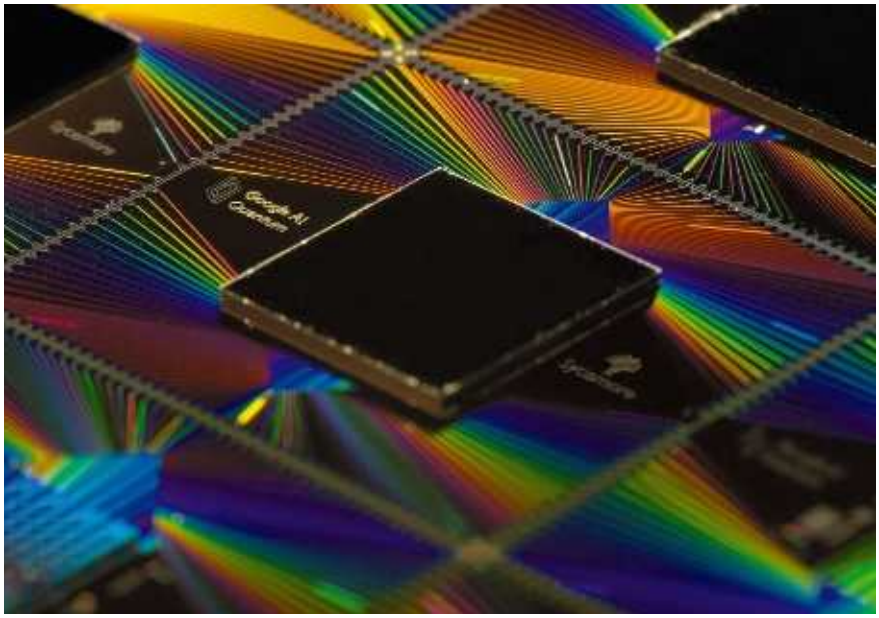
Jiuzhang a réalisé un calcul inutile très difficile à reproduire sur un ordinateur classique

Avec un ordinateur quantique, la résolution du problème est plus simple. Il n'y a pas besoin de faire le calcul laborieux du permanent de la matrice. Il suffit de réaliser le dispositif optique avec les miroirs semi-réfléchissants. Les photons injectés jouent en quelque sorte le rôle des qubits et vont alors « explorer » toutes les possibilités (comme dans l'analogie du labyrinthe). En répétant l'expérience un grand nombre de fois, on obtient la distribution statistique des photons et les probabilités jointes.

À la suite de la proposition de Scott Aaronson et Alex Arkhipov, de nombreux spécialistes pensaient qu'il serait expérimentalement difficile de contrôler assez de photons dans le dispositif imaginé pour atteindre l'avantage quantique. En effet, pour que le système fonctionne, il faut, entre autres, pouvoir générer des photons individuels et indiscernables de façon synchrone. Les physiciens avaient réalisé ce dispositif avec une poignée de photons puis, en 2019, l'équipe de Jian-Wei Pan a développé un système d'échantillonnage de bosons portant sur une dizaine de photons. Les chercheurs ont montré que le calcul classique était difficile pour un ordinateur individuel, mais encore à la portée d'un supercalculateur.

Pour accroître encore le nombre de photons, ils ont utilisé une variante de l'échantillonnage de bosons, l'« échantillonnage gaussien de bosons », qui n'utilise plus des sources de photons uniques. L'« ordinateur quantique » de l'équipe chinoise, nommé Jiuzhang, comporte 100 entrées. Les photons traversent ensuite un circuit de 300 miroirs semi-réfléchissants et 75 miroirs. Ils émergent par l'une des 100 sorties munies d'un détecteur. Les chercheurs ont obtenu la distribution de probabilité de photons en 200 secondes environ. Ils avaient en moyenne 43 photons détectés pour chaque tirage, et un maximum de 76 photons. Ces nombres élevés de particules donnent une idée de la complexité du calcul à traiter par l'approche classique.

Les chercheurs ont estimé que le supercalculateur chinois Sunway TaihuLight (quatrième supercalculateur mondial en novembre 2020) exécutant un algorithme optimisé obtiendrait le même résultat en 2,5 milliards d'années ! De façon générale, les spécialistes saluent le résultat de l'équipe de Jian-Wei Pan. La performance technique est une démonstration forte des progrès de la photonique dans la course à l'ordinateur quantique. Cependant, nombre de chercheurs soulignent que, pour l'instant, une machine comme Jiuzhang n'effectue pas un calcul utile et n'est pas programmable pour résoudre des problèmes concrets – contrairement à la puce Sycamore de Google, qui est un vrai processeur programmable mais limité par son petit nombre de qubits. La course à l'ordinateur quantique continue ! ■



© Google

Le processeur Sycamore qui est au cœur de l'ordinateur quantique de Google manipule 53 qubits. Il est programmable, contrairement au dispositif photonique de l'équipe de Hefei.

SEAN BAILLY

H.-S. Zhong *et al.*, *Science*, en ligne le 3 décembre 2020