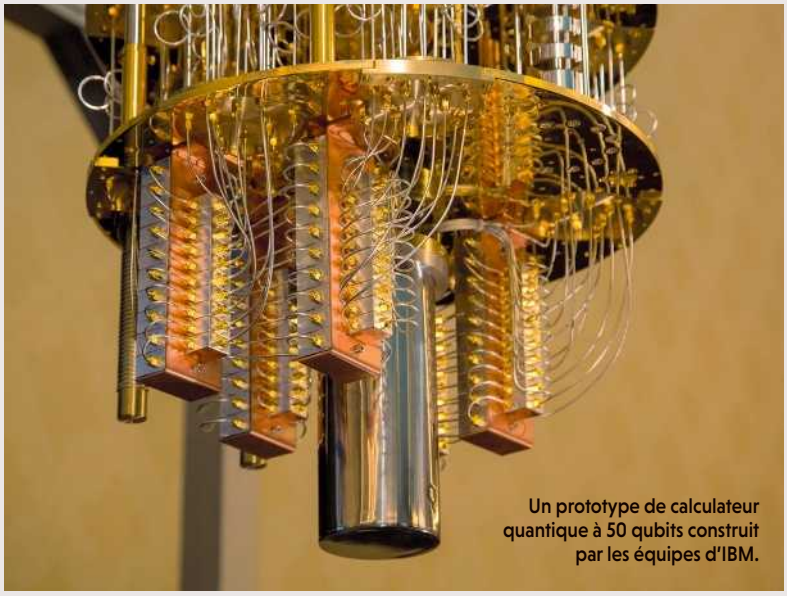
4

LES CALCULATEURS QUANTIQUES



Un prototype de calculateur quantique à 50 qubits construit par les équipes d'IBM.

Depuis vingt-cinq ans, on mène des travaux sur les systèmes de calcul quantique. Ceux-ci, en théorie, seraient capables de calculer plus rapidement que les ordinateurs classiques. Ils utilisent des bits quantiques, ou qubits, au lieu de bits. L'idée repose sur la possibilité de mener, grâce à la superposition quantique, des calculs parallèles en grand nombre et revient à considérer qu'il n'y a pas de limite à l'exactitude de la théorie quantique, même quand elle contredit le principe de densité finie de l'information, lui-même lié à la méfiance que les nombres réels doivent nous inspirer.

L'objectif de la « suprématie quantique » est de mener avec un ordinateur quantique un calcul infaisable avec un ordinateur classique. Il aurait récemment été atteint par Google, mais l'exploit est contesté par les chercheurs d'IBM. Même si l'objectif est atteint, des chercheurs font remarquer que les méthodes envisagées ne produiront rien d'utile, car elles concernent des calculs spécialisés de densités de probabilité qui n'ont pas d'intérêt pratique. Nul n'a prouvé que les recherches concernant les ordinateurs quantiques n'aboutiront pas, mais divers spécialistes, dont Sabine Hossenfelder, physicienne théoricienne à l'institut d'études avancées de Francfort, expliquent qu'il faut rester prudent. Elle écrit : « Quand verrons-nous un ordinateur quantique avec des millions de qubits ? Personne ne sait. Le problème est qu'il est peu probable que les approches dominantes à l'heure actuelle puissent s'adapter pour changer d'échelle. [...] On ne sait pas comment dépasser quelques centaines de qubits. C'est à la fois un problème d'ingénierie et un problème de coût. Cela explique pourquoi, ces dernières années, on a beaucoup parlé des ordinateurs NISQ *(noisy intermediate scale quantum computers)*. Il s'agit en réalité d'un terme inventé pour faire croire aux investisseurs que l'informatique quantique aura des applications pratiques au cours des prochaines décennies. Même s'il est possible qu'on sache prochainement faire fonctionner des NISQ, personne ne sait en tirer quelque chose d'utile. Je ne suis pas très optimiste sur le fait que les ordinateurs quantiques auront bientôt des applications pratiques. Je crains que l'informatique quantique ressemble à la fusion nucléaire ; c'est-à-dire qu'elle reste toujours prometteuse, mais ne fonctionne jamais vraiment. »

> plus vite que la lumière, il semble que les physiciens soient prêts à reconnaître qu'un volume fini d'espace ne peut pas contenir une quantité infinie d'informations.

Les informaticiens Pablo Arrighi, de l'université d'Aix-Marseille et Gilles Dowek, de l'Inria et de l'ENS Paris-Saclay, défendent cette idée d'un principe de densité finie d'information et considèrent qu'il devrait être affirmé clairement, comme celui de la vitesse limitée.

UNE DENSITÉ FINIE D'INFORMATION

Bien sûr, un tel principe empêcherait de croire que la position d'une particule et sa vitesse soient déterminées par des nombres réels dont l'infinité de décimales contient potentiellement une infinité d'informations. Pablo Arrighi et Gilles Dowek proposent une expérience de pensée : « Imaginons une quantité infinie d'informations exprimée sous la forme d'une suite illimitée de 0 et de 1 ; nous pouvons voir cette séquence comme les chiffres d'un nombre réel et écarter les mâchoires d'un pied à coulisse d'une distance correspondant à ce nombre. Cela placerait une quantité infinie d'informations dans un volume fini. Bien sûr, nous avons tous appris que cette idée est absurde et que la distance entre les mâchoires d'un pied à coulisse est fixée avec une précision finie de trois ou quatre chiffres. Il est surprenant que l'affirmation qu'une grandeur physique est toujours définie avec une précision finie n'ait jamais reçu le statut de principe en physique. »

L'idée de ce principe de densité finie d'information, si on savait le rendre précis, aurait une incidence sur les pronostics que l'on fait concernant les capacités futures des ordinateurs quantiques. Le mode de fonctionnement de ces ordinateurs sur lesquels des recherches se poursuivent depuis plus de vingt-cinq ans est la superposition quantique : on obtient dans un volume fini d'espace une grande puissance de calcul en superposant les états quantiques d'un système qu'on fait calculer et qui mène plusieurs calculs en parallèle. Cette possibilité de superposer les calculs est envisagée sans limite et conduirait en théorie à pouvoir dépasser les capacités de calcul des systèmes fondés sur la physique classique.

On sait ainsi comment s'y prendre pour tirer de la mécanique quantique un algorithme fonctionnant en temps polynomial (c'est-à-dire rapidement) pour factoriser les nombres entiers. Cet algorithme conçu par l'Américain Peter Shor en 1995 n'a pas d'équivalent classique connu. Certains systèmes cryptographiques, dont le système RSA notamment utilisé pour les cartes bancaires, s'appuient sur la difficulté de la factorisation. On craint donc que leur sécurité soit mise prochainement en danger.

Pourtant, dès 2003, le logicien Leonid Levin, professeur à l'université de Boston, a exprimé