> chercheurs de Google affirmaient l'avoir atteint. Cet article a depuis été retiré, semant le doute sur la véracité de cette performance. Mais si ce n'est pas le cas, ce n'est sans doute qu'une question de temps. En prévision de ce jour, il est nécessaire de préparer et de bien comprendre ce que signifie la suprématie quantique et si elle a réellement été atteinte. Suivez le guide.

### Qu'est-ce que la suprématie quantique et pourquoi est-ce important ?

Pour atteindre la suprématie quantique, un ordinateur quantique devrait pouvoir effectuer n'importe quel calcul impossible à réaliser en pratique avec un ordinateur classique. En un sens, cette distinction est artificielle. Le test qui sera utilisé pour vérifier la suprématie quantique est un problème *ad hoc* – il s'agit davantage d'un tour de passe-passe que d'une avancée vraiment utile (nous y reviendrons). De fait, les efforts pour construire un ordinateur quantique ne visent pas spécifiquement la suprématie quantique. « Nous n'utilisons pas du tout ce terme; cela ne nous intéresse pas », déclare ainsi Robert Sutor, responsable de la stratégie en informatique quantique chez IBM.

Mais d'un autre point de vue, la suprématie quantique serait un moment décisif dans l'histoire de l'informatique. Elle pourrait en fait conduire à l'avènement d'ordinateurs quantiques qui seraient utiles pour certains problèmes pratiques.

Cet optimisme se justifie au regard de l'histoire. Dans les années 1990, les premiers algorithmes quantiques ont résolu des problèmes artificiels dont personne ne pensait qu'ils étaient vraiment intéressants. Mais les informaticiens qui les ont conçus ont appris des choses qu'ils ont pu appliquer au développement d'algorithmes ultérieurs ayant de grandes conséquences pratiques, à l'image de l'algorithme de Shor, qui sert à factoriser des grands nombres.

« Je ne pense pas que ces algorithmes auraient vu le jour si la communauté ne s'était pas d'abord demandé à quoi peuvent servir en principe les ordinateurs quantiques, sans s'inquiéter immédiatement de leur valeur d'usage », affirme Bill Fefferman, chercheur en information quantique à l'université de Chicago.

La communauté de l'informatique quantique espère que ce processus va se répéter. En construisant un ordinateur quantique qui bat les ordinateurs classiques – même pour résoudre un problème totalement inutile en pratique – les chercheurs apprendront certainement des choses qui leur permettront de construire un jour un ordinateur quantique utile concrètement.

« Avant que nous ayons atteint la suprématie quantique, il n'y a aucune chance qu'un ordinateur quantique puisse faire quoi que ce soit d'intéressant. C'est une étape nécessaire », estime Fernando Brandão, physicien théoricien à l'institut de technologie de Californie et chercheur chez Google.

La suprématie quantique serait en outre un séisme en informatique théorique. Pendant des décennies, ce domaine a tenu pour vraie l'hypothèse de « Church-Turing étendue », selon laquelle un ordinateur classique peut effectuer efficacement tout calcul que tout autre type d'ordinateur peut effectuer efficacement. La suprématie quantique serait la première violation expérimentale de ce principe, et ferait entrer l'informatique dans un tout nouveau monde. « La suprématie quantique serait une percée fondamentale dans la façon dont nous envisageons le calcul », juge Adam Bouland, chercheur en information quantique à l'université de Californie à Berkeley.

### Comment démontrer la suprématie quantique ?

En résolvant sur un ordinateur quantique un problème qu'un ordinateur classique ne peut résoudre de façon efficace. Le problème importe peu, mais on s'attend à ce que la première démonstration de la suprématie quantique porte sur un problème particulier connu sous le nom « d'échantillonnage aléatoire de circuits ».

Un exemple simple est un programme qui simule le lancer d'un dé à 6 faces. Un tel algorithme fonctionne correctement lorsqu'il échantillonne bien les résultats possibles, produisant chacun des nombres de 1 à 6 une fois sur six en moyenne quand on exécute le programme de façon répétée.

À la place du résultat d'un jet de dé, le problème d'échantillonnage aléatoire de circuits consiste à échantillonner les sorties possibles d'un circuit quantique aléatoire. Un circuit peut être vu comme une série d'actions qui peuvent être effectuées sur un ensemble de bits quantiques, ou qubits. Considérons un circuit qui agit sur 50 qubits. Au fur et à mesure que les qubits traversent le circuit, ils peuvent prendre plusieurs états en même temps (ils sont superposés) et se corréler entre eux, c'est-à-dire s'intriquer). Par conséquent, à la fin du circuit, les 50 qubits sont dans une superposition de $2^{50}$ états possibles. Si on mesure les qubits, cet océan de $2^{50}$ possibilités se réduit à une seule chaîne de 50 bits. C'est comme lancer un dé, sauf qu'au lieu de 6 possibilités il y en a $2^{50}$, et que toutes les possibilités n'ont pas la même probabilité.

Les ordinateurs quantiques, qui peuvent exploiter des effets purement quantiques tels que les superpositions d'état, devraient être capables de livrer efficacement à partir de ce circuit aléatoire une série de valeurs de sortie qui reproduit la bonne distribution. Pour les ordinateurs classiques, en revanche, on ne connaît pas d'algorithme rapide pour produire cet échantillonnage – si bien que plus le nombre de

possibilités augmente, plus les ordinateurs classiques sont rapidement dépassés par la tâche.

### Qu'est-ce qui empêche d'atteindre la suprématie quantique pour le moment ?

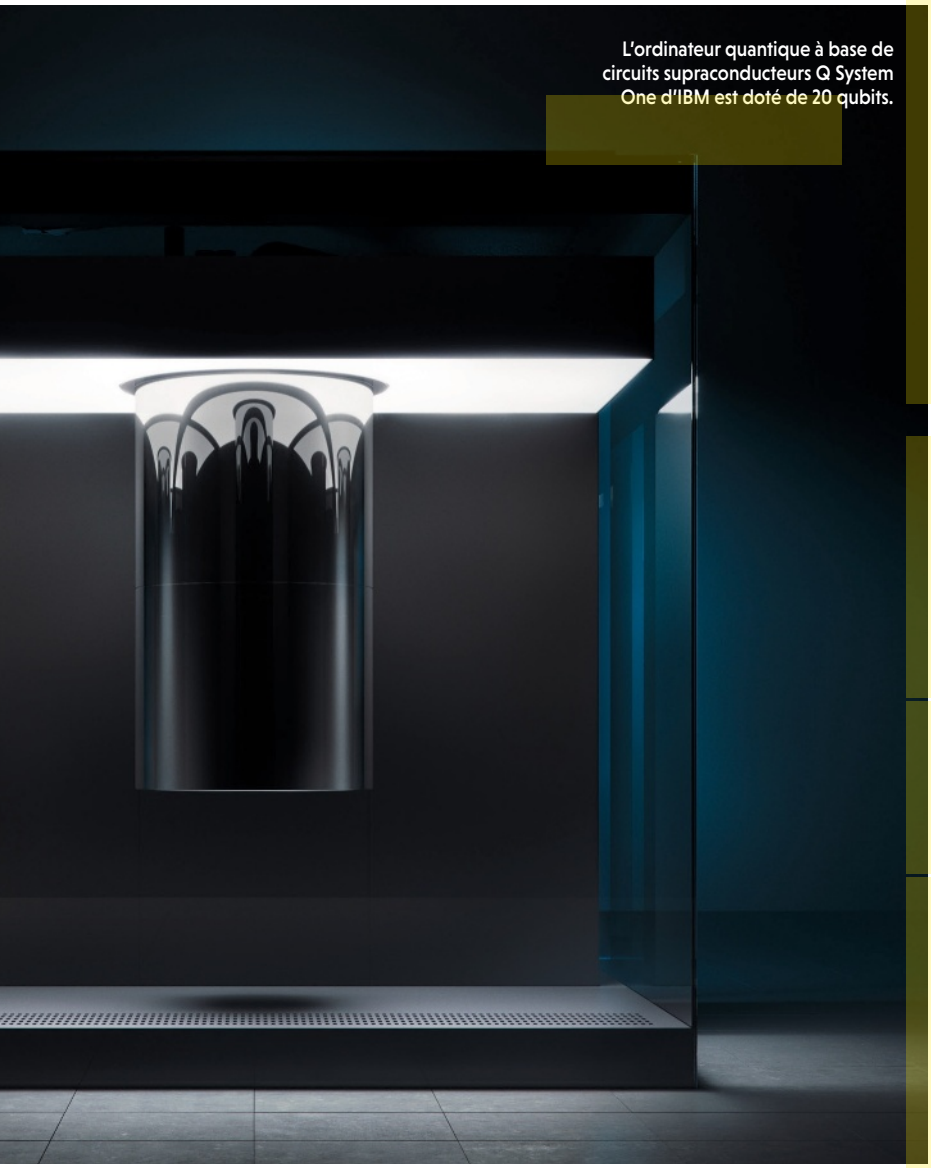
Tant que les circuits quantiques restent petits, les ordinateurs classiques peuvent suivre le rythme. Ainsi, pour démontrer la suprématie quantique par le biais du problème de l'échantillonnage aléatoire des circuits, il faudrait réussir à construire des circuits quantiques plus grands qu'une certaine taille minimale, ce qui n'a pas été le cas jusqu'ici.

La taille du circuit est déterminée par le nombre de qubits de départ combiné au nombre de manipulations sur ces qubits. Dans un ordinateur quantique, les manipulations des qubits sont effectuées à l'aide de « portes logiques », tout comme pour les bits dans un ordinateur classique. Divers types de portes transforment les qubits de différentes façons – certaines font varier la valeur d'un seul qubit, tandis que d'autres combinent deux qubits de telle ou telle façon. Si les qubits passent par 10 portes, on dit que le circuit a une « profondeur » de 10.

Pour atteindre la suprématie quantique, les informaticiens estiment qu'un ordinateur quantique devrait résoudre le problème de l'échantillonnage aléatoire d'un circuit de 70 à 100 qubits avec une profondeur d'environ 10. Si le circuit est beaucoup plus petit, un ordinateur classique pourrait probablement réussir à le simuler – et les techniques de simulation classiques s'améliorent sans cesse.

Mais le problème auquel les chercheurs sont confrontés est que plus le nombre de qubits et de portes logiques augmente, plus le taux d'erreur augmente. Et si le taux d'erreur est trop élevé, les ordinateurs quantiques perdent leur avantage sur les ordinateurs classiques.

Il existe de nombreuses sources d'erreur dans un circuit quantique. La plus cruciale est l'erreur qui s'accumule dans un calcul à chaque fois que le circuit effectue une opération logique. À l'heure actuelle, les meilleures portes quantiques à 2 qubits ont un taux d'erreur d'environ 0,5 %, ce qui signifie qu'il y a environ 1 erreur pour 200 opérations. C'est sans commune mesure avec le taux infime d'erreurs dans un circuit classique, qui est d'environ une erreur toutes les $10^{17}$ opérations. Pour démontrer la suprématie quantique, les chercheurs vont devoir ramener le taux d'erreur des portes à 2 qubits au moins en dessous de 0,1 %.



L'ordinateur quantique à base de circuits supraconducteurs Q System One d'IBM est doté de 20 qubits.

© IBM

### Comment serons-nous certains que la suprématie quantique a été démontrée ?

Certains accomplissements sont sans équivoque. La suprématie quantique n'en fait pas partie. « Ce n'est pas comme le lancement d'une fusée, où il suffit de regarder en l'air pour savoir immédiatement s'il a réussi », explique Scott Aaronson, spécialiste de l'informatique quantique à l'université du Texas à Austin.

Pour vérifier la suprématie quantique, on doit démontrer deux choses : d'une part, qu'un ordinateur quantique a effectué un calcul rapidement, et d'autre part, qu'un ordinateur classique n'aurait pas pu effectuer efficacement ce même calcul.

C'est la seconde partie qui est la plus délicate. Les ordinateurs classiques se révèlent souvent meilleurs pour résoudre certains types de problèmes que ce à quoi s'attendaient les informaticiens. Tant qu'on n'a pas prouvé qu'un ordinateur classique ne peut pas réaliser un calcul efficacement, il existe toujours une possibilité qu'un meilleur algorithme classique, plus efficace, existe. Il ne sera peut-être pas nécessaire de prouver qu'un tel algorithme n'existe pas pour que la plupart des gens soient convaincus par une revendication de suprématie quantique, >

> mais la démontrer solidement pourrait demander encore un certain temps.

**Sommes-nous près d'atteindre la suprématie quantique ?**

Selon de nombreux témoignages, Google frappe à la porte de la suprématie quantique et pourrait la démontrer bientôt. Une annonce avait déjà été faite en ce sens en 2017, avant d'être rétractée, et la nouvelle « annonce » fin septembre 2019 a relancé les spéculations. Mais un certain nombre d'autres équipes ont le potentiel pour atteindre bientôt la suprématie quantique,

## LES ORDINATEURS QUANTIQUES SERONT-ILS TOLÉRANTS AUX PANNES AVANT D'ÊTRE VRAIMENT UTILES ?

notamment au sein des entreprises IBM (*voir Une suprématie contestée, par K. Hartnett également, page 92*), IonQ et Rigetti, ou à l'université Harvard.

Ces équipes suivent plusieurs approches distinctes pour construire un ordinateur quantique. Google, IBM et Rigetti explorent la piste des circuits supraconducteurs. IonQ utilise des ions piégés par des lasers. Le projet de Harvard, dirigé par Mikhail Lukin, utilise des atomes de rubidium. La démarche de Microsoft, qui implique des « qubits topologiques », paraît plus spéculative. Chaque approche a ses avantages et ses inconvénients.

Les circuits quantiques supraconducteurs ont l'avantage d'être constitués d'un matériau solide. Ils peuvent être construits avec les techniques de fabrication existantes, et leurs portes effectuent des opérations très rapides. De plus, les qubits ne bougent pas, ce qui peut être un problème avec d'autres technologies. Mais ces circuits doivent être refroidis à des températures extrêmement basses et chaque qubit d'une puce supraconductrice doit être calibré individuellement, ce qui rend difficile l'adaptation de cette technologie aux milliers de qubits ou plus qui seront nécessaires à un ordinateur quantique utile en pratique.

Les ions piégés offrent un bilan contrasté entre avantages et inconvénients. Ils sont tous identiques, ce qui facilite la fabrication du circuit, et les pièges offrent un temps de stabilité plus long pour effectuer le calcul avant que les états des qubits ne soient submergés par le bruit ambiant (on parle de décohérence). Mais les portes utilisées pour manipuler les ions sont très lentes – des milliers de fois moins rapides que les portes supraconductrices – et les ions individuels peuvent parfois s'échapper des pièges et se déplacer de façon incontrôlée.

À l'heure actuelle, les circuits quantiques supraconducteurs semblent progresser le plus rapidement. Mais de sérieux obstacles d'ingénierie se dressent devant les différentes approches. Une nouvelle avancée technologique majeure sera nécessaire avant qu'il soit possible de construire des ordinateurs quantiques dignes de ce nom. « L'informatique quantique aurait besoin d'une invention analogue au transistor – une technologie révolutionnaire qui fonctionne presque sans faille et qui soit facile à déployer à grande échelle, précise Adam Bouland. Mais bien que les progrès expérimentaux récents aient été impressionnants, mon sentiment est que nous n'avons pas encore trouvé cette clé technologique. »

**Si la suprématie quantique était démontrée, que se passerait-il ensuite ?**

Si un ordinateur quantique atteint la suprématie pour un problème artificiel tel que l'échantillonnage aléatoire de circuits, la question suivante est évidente : quand pourra-t-il faire quelque chose d'utile ?

Le jalon de l'utilité est parfois nommé « avantage quantique ». « Pour une utilisation concrète – comme des services financiers, de l'intelligence artificielle ou de la chimie –, quand et comment pourra-t-on voir un ordinateur quantique faire bien mieux que n'importe quel concurrent classique connu ? », s'interroge Robert Sutor, de chez IBM, dont des clients comme JP Morgan et Mercedes-Benz ont déjà commencé à explorer les applications des puces quantiques IBM.

Un deuxième jalon serait la création d'ordinateurs quantiques tolérants aux erreurs. Ces ordinateurs seraient capables de corriger les erreurs dans un calcul en temps réel, ce qui permettrait en principe de mener des calculs quantiques sans erreur. Mais la principale proposition dans ce sens, connue sous le nom de « code de surface », exige un surcoût massif de milliers de qubits correcteurs d'erreur pour chaque qubit logique utilisé pour un calcul. La tolérance aux erreurs en informatique quantique est donc bien au-delà des capacités actuelles de la technologie. La question de savoir si les ordinateurs quantiques devront être tolérants aux pannes avant de pouvoir être vraiment utiles est ouverte. ■

### BIBLIOGRAPHIE

**J. MARTINIS ET S. BOIXO, Quantum Supremacy Using a Programmable Superconducting Processor, *Google AI Blog*, 2019. http://bit.ly/Goo-Supr**