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