D'année en année, les ordinateurs quantiques semblent régulièrement battre des records. Où en sommes-nous ?

Depuis une dizaine d'années, le rythme s'est accéléré. Un des résultats les plus marquants est probablement l'annonce de Google en 2019, qui a affirmé avoir atteint l'avantage quantique avec son processeur Sycamore contenant 53 qubits physiques. L'avantage quantique (aussi nommé « suprématie quantique ») définit le moment où les supercalculateurs classiques ne sont plus capables de réaliser le calcul d'une machine quantique en un temps raisonnable. La course au nombre de qubits continue : fin 2021, l'université chinoise des sciences et des technologies a présenté Zuchongzhi (62 qubits) et IBM son processeur Eagle (127 qubits).

Pour le grand public, ces annonces donnent peut-être l'impression que l'enjeu autour des ordinateurs quantiques se résume à une question de taille, qu'il suffit d'augmenter le nombre de qubits pour obtenir un dispositif qui fera enfin des calculs vraiment utiles. Le problème est en fait plus complexe, car la performance dépend fortement de la qualité des qubits et de leur connectivité. Selon les critères que l'on regarde, une machine avec seulement quelques qubits « propres » et bien connectés sera parfois plus performante qu'une autre avec davantage de qubits plus bruités.

Par exemple, pour Sycamore, Google a trouvé un bon équilibre, combinant des qubits pas trop bruités, en nombre raisonnable, et bien connectés, ce qui a permis au système de réaliser un calcul, certes complètement inutile, mais *a priori* infaisable par un ordinateur classique.

D'ailleurs, l'avantage quantique revendiqué par Google n'est-il pas contesté ?

Absolument, suite à l'annonce, IBM a contesté la « suprématie » en démontrant qu'en utilisant toute la mémoire du plus gros supercalculateur du monde, le calcul de Google était réalisable en quelques jours seulement. Plus impressionnant de mon point de vue, Xavier Waintal, de l'université Grenoble-Alpes et du CEA, et ses collègues de l'institut Flatiron, à New York, ont montré qu'en utilisant une puissante technique de compression (les réseaux de tenseurs), il était possible de reproduire en quelques heures le calcul de Sycamore sans même recourir à un supercalculateur. Néanmoins, je pense que si Google améliorait son processeur d'un facteur 10 (nombre de qubits, réduction des erreurs, etc.), les machines classiques ne pourraient pas suivre pour ce calcul spécifique.

D'où vient la puissance de calcul des ordinateurs quantiques ?

Dans un ordinateur classique, les transistors fonctionnent déjà grâce à la mécanique quantique. Mais, de façon cruciale, l'information reste portée par un bit qui a un comportement classique et prend soit la valeur « 0 » soit la valeur « 1 ». Dans l'ordinateur quantique, l'information est portée par un bit quantique, ou qubit, qui est une généralisation du bit. Le qubit a intuitivement davantage de degrés de liberté car on autorise une superposition quantique de l'état « 0 » et de l'état « 1 ». Le qubit peut donc être « à la fois » en « 0 » et « 1 », éventuellement même avec des poids complexes (ou amplitudes) différents pour le « 0 » et pour le « 1 ». Le statut physique de ces superpositions reste intensément débattu. Sont-elles réelles ? Sont-elles simplement une représentation mathématique de quelque chose de plus compliqué qui se passe dans le monde réel ? Ce qui compte *in fine* c'est qu'on peut exploiter ce comportement que nous prédit le formalisme quantique pour faire des calculs de manière plus rapide.

On simplifie souvent l'explication de la puissance de l'ordinateur quantique en disant que la superposition explore plus vite l'espace des solutions, en testant toutes les possibilités à la fois. On a par exemple en tête l'image du jeu d'échecs. Pour trouver le meilleur coup, un algorithme classique doit étudier une à une toutes les séquences de coups jusqu'à une certaine profondeur. Intuitivement la superposition permettrait d'explorer toutes les options en même temps, et ainsi de résoudre immédiatement le jeu. En réalité, le gain offert par les superpositions reste minimal pour ce type de problèmes, car il est difficile de lire dans l'état quantique le résultat de cette exploration parallèle.

L'origine de la puissance des ordinateurs quantiques est plus subtile et pas totalement comprise. Elle prend racine dans des interférences entre les qubits du système, qui distinguent les amplitudes apparaissant dans les superpositions quantiques de simples probabilités.

Quelles seraient les applications des ordinateurs quantiques ?

De façon assez naturelle, comme une telle machine est profondément quantique, on s'attend à ce qu'elle soit en mesure de résoudre très efficacement des problèmes de physique quantique tels que le « problème à N corps », c'est-à-dire des systèmes physiques constitués d'une collection de particules en interaction. On aurait alors des applications directes pour étudier les propriétés de nouveaux matériaux, de composés chimiques, de supraconducteurs à haute température, de catalyseurs plus performants, etc. Même si on n'a aucune preuve formelle d'un gain par rapport aux ordinateurs classiques…

Pour ce type de questions, on pourrait d'ailleurs peut-être se satisfaire d'un simulateur

QUELQUES RÉSULTATS RÉCENTS

2022 : QuTech
6 qubits
(spins dans le silicium)

2021 : IBM – Eagle
127 qubits
(supraconducteurs)

2021 : IonQ
32 qubits
(ions piégés)

2021 : université chinoise des sciences et des technologies
62 qubits
(supraconducteurs)

2019 : Google – Sycamore
53 qubits
(supraconducteurs)

quantique analogique. Ces systèmes n'ont pas pour vocation d'être universels comme les ordinateurs mais restent suffisamment configurables pour simuler une variété d'évolutions quantiques apparaissant dans la nature. C'est notamment l'option explorée par Pasqal, une start-up issue de l'institut d'Optique, à Palaiseau. Leur dispositif utilise un ensemble d'atomes neutres piégés dont on peut régler les couplages pour mimer le système physique à simuler.

Plus inattendu, les ordinateurs quantiques sont aussi efficaces pour résoudre certains problèmes qui ne sont pas quantiques par essence, comme la décomposition en facteurs premiers de nombres très grands grâce à l'algorithme proposé en 1994 par le mathématicien Peter Shor du MIT (institut de technologie du Massachusetts).

Les promesses et les attentes sont donc grandes. À quel stade de développement sont les ordinateurs quantiques ?

En 2018, le spécialiste de l'informatique quantique John Preskill qualifiait la période actuelle d'« ère des NISQ » (*noisy intermediate-scale quantum era*), c'est-à-dire l'ère des processeurs dotés de cinquante à quelques centaines de qubits, soumis à pas mal d'erreurs non corrigées, on parle aussi de « bruit ».

Dans un ordinateur classique, on peut avoir des erreurs quand un bit change de valeur (*bit flip* en anglais) : un « 0 » peut accidentellement se transformer en « 1 » et inversement. Les qubits aussi sont susceptibles d'avoir des erreurs. Il existe deux types d'erreurs fondamentales : l'inversion de bit, qui correspond à l'erreur classique, et l'inversion de phase (*phase flip* en anglais), qui est purement quantique.

Ces erreurs proviennent d'interactions avec l'environnement et elles sont beaucoup plus fréquentes dans les systèmes quantiques. Il faut donc protéger le mieux possible les qubits de leur environnement. Mais il est impossible d'isoler totalement un système. Les erreurs se produisent ainsi de façon inéluctable.

Le fait de réaliser un calcul induit-il des erreurs ?

Dans un processeur, classique ou quantique, on veut traiter l'information pour faire des calculs. Pour cela, on utilise des portes logiques qui consistent à inverser la valeur d'un bit, additionner la valeur de deux bits, etc. Ces portes sont réalisées avec des transistors.

Dans l'ordinateur quantique, les portes logiques effectuent aussi des rotations dans l'espace des états du qubit (par exemple l'état initial « 0 » devient une combinaison de « 0 » et « 1 »), ou couplent plusieurs qubits voisins.

Les portes logiques ne sont jamais parfaites et introduisent aussi des erreurs, ne serait-ce que parce que le qubit peut être perturbé par son environnement durant l'opération. Une bonne mesure de la qualité du système est la profondeur atteignable, c'est-à-dire le nombre de portes ou opérations que l'on peut faire sur un qubit avant que le calcul ne contienne presque sûrement une erreur.

Que peut-on faire contre ces erreurs ?

Dans le cas classique, le code correcteur le plus simple repose sur la redondance : encoder un bit logique dans plusieurs bits physiques. Le bit « 0 » est dupliqué en « 000 » et 1 en « 111 ». Ainsi si on mesure plus tard « 010 » et qu'on suppose que les erreurs sont rares, on en déduit que la bonne valeur est 0 avec un « vote de majorité », et on peut rectifier le 1 du milieu en 0. Dans un processeur d'ordinateur classique, les codes correcteurs ne sont pas implémentés car les erreurs sont rarissimes. Ils sont en revanche très utiles quand on fait de la transmission d'information, pour communiquer avec un satellite par exemple.

La correction des erreurs de qubits est bien plus difficile à cause de leur nature quantique et du problème de la mesure. Quand on mesure la valeur d'un qubit dans une superposition d'états, on provoque l'effondrement de cette superposition et on n'observe qu'un seul des états possibles. La moindre fuite d'information (comme l'émission d'un photon) qui nous renseignerait sur le système conduit à la destruction de la superposition. Or il faut préserver la superposition des états des qubits tout au long du calcul pour que celui-ci aboutisse. On ne peut ainsi pas simplement mesurer les qubits physiques pour savoir si une erreur s'est produite et la rectifier.

Quelle est alors la solution ?

La solution consiste toujours à encoder l'information d'un qubit dit « logique » de manière redondante dans un plus grand nombre de qubits physiques. L'idée est ensuite de faire d'astucieuses mesures globales qui nous disent si le système contient une erreur (on parle de « syndromes d'erreurs ») et comment la corriger. Ces syndromes sont conçus intelligemment pour ne pas faire fuir d'information sur l'état de superposition du qubit lui-même lorsqu'ils sont mesurés. Pour l'implémentation de ces approches, on fait appel à des codes correcteurs quantiques dont il existe différents types (*voir* Calculer plus vite… et sans erreur ? *page 31*). Un point essentiel est qu'un code correcteur demande toujours une redondance, on utilise plusieurs qubits physiques pour une unité d'information quantique (le qubit logique). Plus on veut réduire les erreurs, plus le rapport du nombre de qubits physiques sur le nombre de qubits logiques (en anglais l'*overhead*) augmente.

La société Alice&Bob explore la piste de qubits de chats, des qubits supraconducteurs dans lesquels il est possible d'éliminer un type d'erreurs. Ici, la puce est intégrée dans le dispositif, qui permet de la connecter et de la refroidir, afin d'en mesurer les caractéristiques.

© Further Studio/Nil Hoppenot