

Pouvez-vous nous rappeler ce qu'est un ordinateur quantique ?

C'est une machine «intriquante», c'est-à-dire un dispositif qui exploite la possibilité de superposer et d'intriquer les états quantiques de plusieurs systèmes physiques – c'est-à-dire de les lier de façon très étroite, spécifique à la physique quantique – afin de mettre en œuvre des calculs hors de portée des ordinateurs actuels.

D'où vient la puissance calculatoire particulière que vous évoquez ?

Pour le faire ressentir, j'aime bien utiliser cette métaphore : rechercher la solution d'un problème revient à essayer de faire traverser un labyrinthe complexe par un personnage.

Si c'est un ordinateur classique qui aide ce personnage, il lui fera, à chaque embranchement, essayer toutes les voies, rebrousser chemin au bout de chaque cul-de-sac, puis recommencer jusqu'à trouver la sortie. Il se peut que, par chance, le personnage trouve vite comment traverser, mais il se peut aussi qu'il meure avant que l'exploration systématique ne lui ait révélé la sortie du labyrinthe...

Si c'est un ordinateur quantique qui assiste le personnage, il le «superposera», à chaque embranchement, à un *alter ego* qui explorera l'autre voie. En d'autres termes, on aura simultanément l'état représenté par le personnage allant à gauche et l'état d'un *alter ego* allant à droite. Résultat : en une passe, l'ordinateur quantique fait essayer en parallèle toutes les voies au personnage. Il construit ainsi un état qui superpose tous les états d'*alter ego* effectuant tous les parcours possibles, y compris celui qui permet de traverser. Un témoin présent à la sortie permettra alors d'extraire, parmi la multitude d'*alter ego*, celui qui aura traversé le labyrinthe – autrement dit la solution au problème posé.

Cela revient en somme à une forme de parallélisme massif...

Exactement, un parallélisme massif et inhérent à une propriété subtile du monde quantique : l'existence d'états qui sont des superpositions de plusieurs états quantiques de base d'un certain système physique. Une autre façon de paralléliser consiste à «intriquer» l'état d'un système physique avec celui d'un autre, l'intrication étant un lien spécifiquement quantique, qui subsiste quelle que soit la distance séparant les deux systèmes. J'insiste sur un point : puisqu'il fonctionne sur un principe différent, l'ordinateur quantique ne remplacera pas l'ordinateur classique, mais il le complétera quand un problème sera hors de sa portée...

Quels types de problèmes dépassent l'ordinateur classique ?

Si nous disposions d'un ordinateur quantique, nous pourrions, de manière générale, résoudre

bien plus vite tous les problèmes d'optimisation, ceux où il faut rechercher une solution parmi un très grand nombre de possibilités. Par exemple, cette capacité pourrait nous aider à développer bien plus vite des molécules thérapeutiques, à réaliser des simulations pour trouver enfin la formule d'un supraconducteur à vraiment haute température, à faire de meilleures prévisions météorologiques, à optimiser les investissements financiers, etc.

Mais l'exemple emblématique est un problème arithmétique : avec un ordinateur quantique, on pourrait décomposer un très grand nombre en ses facteurs premiers beaucoup plus vite. Cela bouleverserait la cryptographie, puisque la sécurité du chiffrement RSA, le plus utilisé aujourd'hui, repose sur l'impossibilité, avec un ordinateur classique, d'effectuer la même tâche en un temps raisonnable.

Et où en sommes-nous ? Quels sont les obstacles à surmonter pour construire un ordinateur quantique ?

Vaste question ! Disons pour commencer que les théoriciens qui développent l'algorithmique quantique supposent de pouvoir disposer d'un certain nombre de bits quantiques, ou qubits (pour *quantum bits*). Un qubit est l'équivalent concret du personnage superposable que j'évoquais plus haut. Un bit classique ne peut valoir que 0 ou 1. Un qubit, lui, a deux états de base notés $|0\rangle$ et $|1\rangle$, et il peut être dans une superposition des deux, c'est-à-dire dans un état de la forme $a|0\rangle + b|1\rangle$. Ensuite, l'étape de calcul va créer des liens d'intrications multiples entre différents qubits, liens qui contribuent au parallélisme et permettent d'aboutir au résultat très efficacement.

Un ordinateur quantique consiste donc en un étage constitué d'un ensemble de qubits et en un étage qui effectue un calcul ?

Oui, comme dans un ordinateur classique, dans un ordinateur quantique, le calcul suppose l'assemblage d'un certain nombre de portes logiques, mais les portes logiques quantiques intriquent les qubits entre eux... Aujourd'hui, la difficulté technique essentielle à franchir pour obtenir un ordinateur quantique est triple : 1) disposer d'un grand nombre de qubits ; 2) parvenir à les combiner en des états intriqués ; 3) maintenir la cohérence de ces états assez longtemps pour que les calculs puissent aller à leur terme.

Ainsi, il faut d'abord avoir des qubits. Par quelles techniques y parvient-on ?

Il en existe de l'ordre d'une vingtaine, je crois, mais quatre filières font l'objet d'un développement intense. La plus avancée est celle des ions piégés, dans laquelle deux groupes mènent la course en tête : celui de Rainer Blatt, à >

> L'université d'Innsbruck, en Autriche, et celui de Chris Monroe, à l'université du Maryland, aux États-Unis.

La technologie des ions piégés est la mise en pratique de nos anciennes expériences de pensée de physique quantique: on réalise des dispositifs où des champs électriques et magnétiques piègent des ions disposés en série les uns à côté des autres; chaque ion, *via* l'état d'énergie d'un électron, constitue un qubit. Une impulsion laser appropriée permet de modifier l'état électronique d'un ion, pour en faire une superposition des états $|0\rangle$ et $|1\rangle$. Ensuite, l'enjeu est de construire des portes logiques quantiques qui, en pratique, intriquent les états des ions entre eux en jouant sur leurs fréquences d'oscillation dans leur piège commun.

Cette filière est très avancée puisque, pour faire des calculs, on dispose de temps de cohérence de quelques minutes, ce qui est très long. En théorie, cela permet d'empiler beaucoup de portes logiques... ce qui veut dire beaucoup d'opérations.

Combien de qubits contiennent les ensembles d'ions piégés que l'on a obtenus ainsi ?

Des annonces tapageuses dans les médias ont fait état de 70 qubits, mais seul est pertinent le nombre de qubits que l'on peut combiner tout en maintenant la cohérence quantique assez longtemps pour réaliser un calcul. De ce point de vue, le bon chiffre serait plutôt entre une quinzaine et une vingtaine... ce qui est aussi vrai des autres filières avancées d'aujourd'hui, que celles-ci exploitent des atomes ou des atomes artificiels.

Des atomes artificiels ? C'est-à-dire ?

Dans la filière des ions piégés, les qubits sont des états d'énergie d'électrons atomiques. Dans les autres filières dominantes, il s'agit aussi d'états d'énergie d'électrons, mais d'électrons liés à des «atomes artificiels», c'est-à-dire à de petits dispositifs microscopiques conçus pour lier une telle particule. Dans deux des autres filières, par exemple, les électrons sont liés soit au sein de petites boucles de courant en milieu supraconducteur, soit au sein de «boîtes quantiques» réalisées dans du silicium – de minuscules structures où l'électron est confiné.

Tandis que Google et IBM mènent la danse dans la première filière, des équipes des Pays-Bas, d'Australie et des États-Unis la mènent dans la deuxième. Des chercheurs du CEA et du CNRS à Grenoble s'y sont aussi lancés en 2016. Bref, dans ces filières, on a reconstitué au sein d'atomes artificiels l'équivalent d'une échelle des états d'énergie d'électrons atomiques. La très grande subtilité technique de la construction et du maintien en cohérence

des superpositions d'états en milieu solide a limité jusqu'à présent le nombre de qubits atteint: il est d'environ 20 dans le cas des dispositifs supraconducteurs, et de 2 dans le cas des boîtes quantiques en silicium...

Seulement 2 ? Pourquoi alors poursuivre dans cette voie ?

Ce nombre modeste de qubits du côté du silicium reflète le grand défi à relever pour que cette technologie soit viable: trouver le moyen d'augmenter le nombre de qubits intriqués. Pour autant, comme cette filière s'appuie sur la technologie CMOS qui sert à produire les microprocesseurs actuels, son potentiel industriel est grand et il est donc important de l'explorer. Si l'on parvenait à intriquer un grand nombre de qubits réalisés en semi-conducteurs, on aurait toute facilité pour les produire par millions...

Mais les intriquer en grand nombre ne suffit pas; ne faut-il pas aussi réussir à conserver la cohérence des états correspondants ?

Oui, il y a aussi un défi du côté de la cohérence, comme dans tout système à l'état solide, mais le défi est aussi du côté de la «connectivité», c'est-à-dire la capacité à intriquer des qubits qui sont distants les uns des autres. Pour l'instant, l'état de l'art avec le silicium consiste à intriquer une boîte quantique avec sa plus proche voisine seulement !

Il faut maintenir la cohérence quantique assez longtemps pour réaliser un calcul

Existe-t-il une autre filière où l'on peut espérer intriquer un grand nombre de qubits sans perdre trop rapidement leur cohérence ?

La mienne, peut-être, qui est celle de l'ordinateur quantique optique. Dans cette voie, les qubits sont par exemple les états de polarisation de photons uniques, photons que l'on combine en les introduisant simultanément à l'entrée d'un circuit optique effectuant le calcul. Les portes logiques quantiques peuvent être réalisées à base de miroirs, de lames