

et d'autres plutôt «pratiques», et donc banales. Je pense qu'apporter au monde réel quelque chose d'utilisable par tout le monde n'est jamais banal. C'est extrêmement difficile. Il y a un bond de géant entre: «J'ai une idée géniale, par exemple un écran tactile, discutons-en sur le tableau blanc» et le smartphone que j'utilise actuellement. Avec l'internet quantique, nous sommes dans la même situation, nous essayons de le construire en partant de rien.

Nous partons d'une expérience préliminaire en laboratoire pour essayer de mettre en place un système étendu à tous les Pays-Bas, fonctionnant à distance et utilisable par des individus, qui, à terme, n'auront pas besoin de s'y connaître en physique pour le faire. Si une partie du système existait déjà, nous pourrions simplement dire «améliorons-la». Mais créer *ex nihilo* est une autre affaire. Passer de rien à une première version est très long.

En faisant cela, je pense que nous accéderons à une compréhension plus fondamentale dans plusieurs domaines. Nous en apprendrons plus sur la physique en rendant

possibles ces réseaux parce que, actuellement, nous ne savons pas exactement comment le faire. Nous testons encore différents types de nœuds et de répéteurs quantiques, des appareils qui relaient l'intrication sur de plus grandes distances. Et, dans le domaine des sciences informatiques, nous découvrons de nouvelles façons de programmer et contrôler de tels réseaux grâce aux différences fondamentales qui existent entre les communications quantique et classique.

Mais je pense aussi que nous obtiendrons des informations sur les processus créatifs et la sociologie en suivant la façon dont les usagers s'empareront de ces nouveaux réseaux. Souvenez-vous des débuts de l'internet classique, la plupart pensaient qu'il ne servirait qu'à envoyer des fichiers un peu partout. Mais la société a fait preuve de bien plus d'imagination !

Il est difficile de définir un calendrier, mais espérez-vous voir de votre vivant cet internet quantique ?

Stephanie Wehner : Je suis assez optimiste à ce propos, je pense que oui. ■

BIBLIOGRAPHIE

G. MURTA ET AL., Towards a realization of device-independent quantum key distribution, *Quantum Physics*, 2019.
<https://arxiv.org/abs/1811.07983>

S. WEHNER ET AL., Quantum internet: A vision for the road ahead, *Science*, vol. 362(6412), eaam9288, 2018.

D. CASTELVECCHI, The quantum internet has arrived (and it hasn't), *Nature*, vol. 554(7692), pp. 289-292, 2018.

S. WEHNER ET AL., Cryptography from Noisy Storage, *Phys. Rev. Lett.*, vol. 100, 220502, 2008.

Que sais-je?

100 MOTS

100% ASTRONOMIE

LES 100 MOTS DE L'ASTRONOMIE

INÉDIT

100 MOTS DE L'ASTRONOMIE

Jean Audouze

Que sais-je?

EN LIBRAIRIE

PASCALE SENELLART- MARDON



« Les Chinois ont mis un grand coup d'accélérateur avec des moyens considérables »

En quelques mots, qu'est-ce qu'un ordinateur quantique ?

Pascale Senellart-Mardon : 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 (voir *Pas d'échappatoire pour l'intrication*, par R. Hanson, page 26) – 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 ?

Pascale Senellart-Mardon : 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 à un personnage. Si c'est un ordinateur classique qui aide

BIO EXPRESS

Pascale Senellart-Mardon est directrice de recherche au CNRS et chercheuse au Centre de nanosciences et de nanotechnologies du CNRS et de l'université Paris-Saclay.

Elle a cofondé la société Quandela (grand prix i-Lab 2018), qui produit des sources de photons pour ordinateurs et communications quantiques.

ce personnage, il lui fera, à chaque embranchement, essayer successivement 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 « superpose », 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 étape, 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...

Pascale Senellart-Mardon : 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 complètera quand un problème sera hors de sa portée...

Quels types de problèmes dépassent l'ordinateur classique ?

Pascale Senellart-Mardon : 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...

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 ?

Pascale Senellart-Mardon : 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'étage de calcul va créer des liens d'intrications multiples entre

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 $|1\rangle$.

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

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 ?

Pascale Senellart-Mardon : 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 ?

Pascale Senellart-Mardon : 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 :

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 ainsi obtenus ?

Pascale Senellart-Mardon : 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 ?

Pascale Senellart-Mardon : 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 ➤