

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'étape 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 ➤