

Mazyar Mirrahimi, Inria : « Un ordinateur quantique dans dix ans ? Impossible de l'affirmer »

Saint Graal, utopie, devenir de l'informatique : l'ordinateur quantique est l'objet de beaucoup de fantasmes. Que se cache-t-il derrière cette appellation ? Quels sont les travaux menés et quelles avancées ont été réalisées ? Quels obstacles rencontre-t-on encore dans le développement d'un ordinateur quantique universel, présenté comme le successeur de nos machines au silicium ? Les réponses de Mazyar Mirrahimi, chercheur à l'Inria (Institut national de recherche en informatique et en automatique).

Silicon.fr : Comment expliquez-vous l'engouement autour de l'informatique quantique ?

Mazyar Mirrahimi : L'enthousiasme actuel s'explique par les perspectives touchant au développement d'ordinateurs universels quantiques, capables de résoudre des problèmes non accessibles à des ordinateurs classiques, comme la factorisation de grands nombres utilisée par les algorithmes de cryptage. Mais très certainement d'autres applications verront le jour avant l'apparition d'un tel calculateur universel. A titre d'exemple, on devrait assister dans les années à venir au développement de simulateurs quantiques permettant de tester divers modèles physiques dont la simulation n'est pas réalisable par un ordinateur classique. Cela pourrait même mener à prédire de nouveaux phénomènes physiques auxquelles nous ne pensons pas aujourd'hui. Enfin, comme dans le développement de toute autre technologie, je pense que les applications qui seront les plus marquantes dans le futur restent difficiles à prédire aujourd'hui.



Est-ce la voie suivie par la société canadienne D-Wave (qui conçoit des ordinateurs quantiques spécialisé dans les algorithmes d'optimisation) ?

M.M. : C'est encore une autre voie : on parle ici de calcul quantique adiabatique. Il s'agit de systèmes spécialisés dans les problématiques d'optimisation : certaines de ces dernières sont formulées en tant que problèmes de recherche d'un état d'énergie minimum d'un système quantique. Sur ce terrain, beaucoup reste à faire du côté théorique et expérimental pour affirmer que ces machines amènent de vrais bénéfices en termes de temps de calcul par rapport aux ordinateurs classiques. A ma connaissance, les machines D-Wave achetées aujourd'hui servent en grande partie à la recherche et l'analyse comparative de leurs capacités.

Est-on assuré aujourd'hui de parvenir à développer un jour un ordinateur quantique universel ?

M.M. : Il y a 20 ans, cela paraissait bien plus difficile qu'aujourd'hui. Mais, depuis, les chercheurs ont effectué des percées impressionnantes. Plusieurs pistes de recherche sont explorées en parallèle,

sur la base des mêmes principes physiques fondamentaux. Toutes visent à développer des outils qui peuvent être vus comme les composants d'un futur ordinateur quantique universel.

Il reste toujours des obstacles importants à surmonter. Il est impossible d'affirmer avec certitude que nous disposerons dans dix ans d'un ordinateur quantique universel, même si, à cette échéance, je suis persuadé qu'il existera une technologie d'information quantique ouvrant la porte à de nouvelles avancées.

A quelles difficultés se heurte-t-on ?

M.M. : Résoudre des problèmes non accessibles aux calculateurs actuels implique d'être en mesure de manipuler des milliers de qubits (unité de stockage de l'information en informatique quantique, ainsi dénommée par analogie au bit, NDLR). Or, la superposition quantique (la caractéristique centrale de l'informatique quantique, par laquelle un qubit peut en même temps valoir 0 et 1) est très fragile. L'interaction non-contrôlée d'un qubit avec son environnement mène à une destruction rapide de ces états de superposition : c'est ce qu'on appelle le problème de décohérence. Plusieurs voies sont aujourd'hui explorées pour tenter de dépasser cette limite. La première consiste à améliorer l'isolation du qubit par rapport à son environnement et au 'bruit' qu'il génère ou de le rendre insensible à certaines sources de bruit. C'est grâce à ces techniques que des avancées majeures ont eu lieu avec les qubit supraconducteurs. Elles se traduisent par une amélioration importante du temps de vie d'un qubit : on est ainsi passé de l'ordre de la nanoseconde en 1999 (première réalisation d'un tel qubit) à 100 microsecondes aujourd'hui. Soit une multiplication par 100 000. Ensuite, les chercheurs tentent de mettre au point des méthodes actives de correction d'erreur. En s'inspirant des méthodes de correction d'erreur en informatique classique. L'idée consiste à encoder l'information de façon redondante, en utilisant par exemple plusieurs qubits à la place d'un seul. Je pense qu'il s'agit là de l'étape clef à franchir dans la mise au point du premier ordinateur quantique universel.

Récemment, une [expérience menée par les équipes de John Martinis](#), de l'université de Californie (équipes auxquelles Google est associé depuis septembre dernier, NDLR), laisse entrevoir une percée dans la correction d'erreurs. Qu'en pensez-vous ?

M.M. : Dans cette expérience récente, le groupe de John Martinis manipule 9 qubits avec des durées de vie intéressantes sur une seule puce. Cette expérience, comme quelques autres menées par d'autres groupes actifs dans ce domaine, représentent des étapes importantes vers la réalisation de la correction d'erreur quantique. Toutefois, l'expérience mentionnée traite seulement le cas de la détection d'un seul type d'erreur dite « flip de bit » et ne permet pas la correction de ces erreurs en temps réel. Elle peut être vue comme une preuve de principe de la faisabilité d'une telle correction d'erreur, mais la réalisation d'un code correcteur d'erreur quantique complet reste à faire.

Et cette problématique de gestion des erreurs ne fait que croître à mesure qu'augmente le nombre de qubits ?

M.M. : Tout à fait. Certes, D-Wave manipule 512 qubits sur ses systèmes, mais ces unités logiques ont une durée de vie très limitée et ne présentent pas de caractéristiques intéressantes pour le développement d'un ordinateur universel.

Pour reprendre l'exemple précédent, aller au-delà de 9 qubits implique une augmentation du risque d'apparition de nouvelles sources de bruits, en particulier, de bruits corrélés (qui peuvent affecter plusieurs qubits à la fois). Nous parlons ici du problème de « scalabilité » : comment augmenter la taille du système de façon significative sans détériorer les propriétés de ses sous-systèmes ? C'est le cœur du problème dans le développement d'un ordinateur quantique universel.

Vous dirigez l'équipe Quantic de l'Inria. Sur quels sujets travaillez-vous ?

M.M. : Notre équipe d'une douzaine de personnes, dont 5 permanents, est une équipe commune entre l'Inria, l'ENS (Ecole Normale Supérieure), le CNRS, l'université Paris VI et Mines Paristech. La recherche expérimentale sur les circuits supraconducteurs est localisée à l'ENS. Dans le cadre de nos recherches, nous collaborons aussi avec d'autres groupes à l'avant-garde du domaine, comme le laboratoire Kastler-Brossel de l'ENS, l'université de Yale, et le CEA Saclay.

Parmi les activités variées de notre équipe, je peux en citer deux, qui s'avèrent centrales. Un premier axe de recherche concerne le contrôle par rétroaction de systèmes quantiques. Il s'agit d'un sujet central dans la problématique de la correction d'erreur quantique. En effet, ce problème de correction d'erreur est équivalent à la stabilisation d'une variété d'états quantiques ou toute dérive par rapport à cette variété doit être compensée en temps réel.

Le deuxième axe concerne le développement des outils du calcul quantique universel efficace en matériel. L'idée est d'utiliser un grand nombre de photons d'un champ électromagnétique pour encoder l'information de façon redondante. En explorant les niveaux d'énergie plus élevés d'un seul système quantique, nous évitons alors la nécessité d'utiliser plusieurs qubits (systèmes à deux niveaux d'énergie) pour atteindre un code correcteur d'erreur.

Ces dernières années, IBM, Google ou encore Microsoft ont investi massivement dans le domaine. Ne court-on pas le risque de voir l'Europe dépassée faute de financements suffisants ?

M.M. : Effectivement, les avancées impressionnantes sur les circuits supraconducteurs quantiques depuis 15 ans ont mené ces sociétés à y investir massivement. Et il n'y a pas, à ma connaissance, de société européenne consacrant autant de ressources au sujet. Mais la recherche européenne sur le sujet est très active. Et le continent compte quelques start-up dans le domaine voisin de la communication quantique.

A lire aussi :

[Ordinateur quantique : Google apprend à corriger quelques erreurs](#)

[Une première dans l'intelligence artificielle « quantique » ?](#)

[Ordinateur quantique : Microsoft et Alcatel-Lucent sont-ils sur la bonne piste ?](#)

Crédit Photo : Welcomia-Shutterstock