



FSMP
Fondation Sciences
Mathématiques de Paris

MATHSINFOS L'ORDINATEUR QUANTIQUE

Un concept révolutionnaire

Le concept d'ordinateur quantique met en jeu de nouvelles règles de calcul basées sur les superpositions d'état et l'*intrication* (la dépendance mutuelle des états quantiques de particules distantes), et est devenu l'objet de recherches intenses dans le champ académique, avec une implication forte - et croissante - de grandes compagnies industrielles. Au niveau conceptuel, le principe de fonctionnement d'un ordinateur quantique est effectivement révolutionnaire. Des théoriciens de l'information, de l'algorithmique, et de la théorie de la complexité se sont alors emparés des lois de la physique quantique pour imaginer de nouveaux algorithmes et de nouvelles architectures de calcul, basées sur des « portes logiques quantiques » sans équivalent classique. Cette rencontre entre la théorie de l'information et la mécanique quantique renouvelle les outils théoriques utilisés de part et d'autre, et suggère aussi de nouvelles approches des fondements de la théorie quantique.

Qubit, difficultés pratiques

De nombreux systèmes quantiques sont étudiés en tant que support de l'unité quantique d'information, le « qubit ». Un qubit peut être soit dans l'état zéro soit dans l'état un, comme un bit classique, mais aussi dans une superposition quantique cohérente de ces deux états. Il faut de plus pouvoir utiliser l'intrication, en créant des superpositions quantiques de registres contenant plusieurs qubits. Les supports des qubits peuvent être des objets physiques « naturels » (photons, atomes ou ions), mais se développent aussi des qubits « artificiels », comme les systèmes supraconducteurs à quantum de flux ou de charge. Un enjeu majeur est d'assembler un grand nombre de qubits en conservant leurs propriétés de cohérence. Ceci requiert l'utilisation de codes correcteurs quantiques, et le nombre de qubits disponibles dans les systèmes les plus avancés (jusqu'à une vingtaine) devrait permettre une démonstration de principe de ces codes dans un futur proche. L'assemblage cohérent de qubits à très grande échelle demeure néanmoins un obstacle majeur à franchir, et même si un appareil est commercialisé par la compagnie canadienne DWave, une réelle « accélération quantique » (quantum speed-up) dans un calcul n'a pas encore été démontrée de manière convaincante.

La mécanique quantique a été une révolution scientifique majeure du XX^e siècle. Basée sur le concept de « dualité onde-particule », la première révolution quantique a d'abord permis de comprendre la structure de la matière. Elle a ensuite conduit au transistor et à la micro-électronique, au laser et aux télécommunications optiques, aux horloges atomiques et au GPS : bref, à tous les outils technologiques de la société de l'information et de la communication. Mais à partir des années 1960, une nouvelle révolution quantique a émergé, qui ne concerne plus seulement le comportement statistique d'un très grand nombre d'objets élémentaires - électrons, atomes ou photons - mais le comportement individuel d'un petit nombre d'objets quantiques. Elle est liée au développement de techniques expérimentales extraordinaires qui ont permis de capturer, observer, contrôler des électrons, des ions ou des atomes uniques, et d'émettre des photons un par un. Il est alors apparu que ces objets peuvent être « intriqués », et ce comportement étonnant, discuté auparavant dans des expériences de pensée, est devenu l'objet d'investigations expérimentales et théoriques. Cette seconde révolution quantique est maintenant sollicitée pour ouvrir la porte à l'*information quantique*.

Selon la célèbre maxime de Rolf Landauer, « l'information est de nature physique ». Un support quantique de l'information doit donc permettre la transmission et le traitement quantique de cette information, avec des règles du jeu différentes de celles que l'on connaît en physique classique. On a alors accès, comme nous le verrons dans ce numéro, à de nouvelles méthodes de cryptographie dont la sécurité s'appuie sur les lois fondamentales de la physique, ou à de nouvelles méthodes de calculs qui peuvent être exponentiellement plus efficaces.

L'ordinateur quantique associe un concept vraiment nouveau (l'information quantique ne se manipule pas comme l'information classique, et cette différence est potentiellement utile), et le développement de technologies qui s'efforcent de devenir une ingénierie quantique, et dont la mise en œuvre pratique progresse remarquablement, mais lentement. Cette possibilité attire l'intérêt de nombreux mathématiciens, physiciens, informaticiens, biologistes... et aussi des grandes compagnies de l'informatique, par exemple ATOS en France. En parallèle, les nouvelles technologies quantiques résultant de ces études sont déjà utilisées pour atteindre voire contourner les limites standard en métrologie des temps ou des fréquences, des longueurs ou des angles, de la gravitation, des champs magnétiques... Pour soutenir l'ensemble de ces recherches, la Commission Européenne a décidé lancer un Quantum Technology Flagship, associant des financements Européens et nationaux, et aussi des équipes académiques et industrielles. En région Île-de-France, une centaine d'équipes sont concernées, et sont regroupées dans un projet DIM (Domaine d'Intérêt Majeur) intitulé SIRTEQ (Science et Ingénierie en Région Île de France pour les Technologies Quantiques).

*Alain Aspect et Philippe Grangier
Laboratoire Charles Fabry, Institut d'Optique Graduate School, Université Paris-Sud*

Simulateurs quantiques

Au stade actuel, on peut penser que les premiers résultats utiles du calcul quantique viendront des simulateurs quantiques, proposés par Feynman dans son article fondateur de 1982. Il s'agit de laisser la nature calculer pour nous, en réalisant des expériences sur des systèmes parfaitement contrôlés, par exemple des atomes ultra-froids placés dans des potentiels lumineux. Suivant la structure périodique ou désordonnée de ces potentiels, les atomes simulent la physique de systèmes difficiles à étudier directement, qui peuvent aller des électrons dans des matériaux complexes, jusqu'à la matière constituant une étoile à neutrons.



FSMP
Fondation Sciences
Mathématiques de Paris



Paris Centre for Quantum Computing

Paris Centre for Quantum Computing (PCQC) est une Fédération de Recherche CNRS fondée en 2014 qui rassemble plus de vingt informaticiens, mathématiciens et physiciens théoriciens et expérimentaux, de Paris et de ses environs, autour du traitement de l'information quantique. Leur objectif est de développer de nouvelles technologies quantiques d'information et de communication et de tracer la voie menant du PC au QC, c'est-à-dire de l'ordinateur personnel tel qu'il existe actuellement à l'ordinateur quantique. Les équipes de recherche de PCQC sont interdisciplinaires, avec des chercheurs issus de ses institutions partenaires : CNRS, Université Paris-Diderot, Université Pierre et Marie Curie, Télécom ParisTech, Inria Paris, CEA, Institut d'Optique, Université Paris-Sud. C'est la nécessité de cette approche pluridisciplinaire qui a motivé la création de PCQC, pour permettre à ses membres de collaborer et de partager leurs ressources, mais aussi d'accroître leur visibilité et leur attractivité internationales. Les journées bi-annuelles **Quantum In Paris (QuPa)** rassemblent largement les diverses communautés représentées par PCQC.

Les objectifs de PCQC incluent aussi animation, valorisation, et interaction avec des industriels. Récemment, PCQC a signé un contrat de collaboration industrielle via l'appel « Grand défis du numérique » du PIA3 avec d'autres partenaires académiques ainsi que Airbus Group, CryptoExperts, CS Systèmes d'Information, Gemalto, Secure-IC S.A.S, THALES, de même qu'un MoU avec les deux autres principaux centres européens en calcul quantique, University of Latvia et University of Amsterdam.

Mathématiques en Mouvement sur l'ordinateur quantique

L'édition 2017 de *Mathématiques en Mouvement*, organisée par la FSMP avec Mathematic Park, a eu pour thème : *L'ordinateur quantique*. Auteurs des exposés présentés lors de cette journée, André Chailloux (SECRET, Inria Paris), Eleni Diamanti (LIP6, CNRS, Université Pierre et Marie Curie), Sophie Laplante (IRIF, Université Paris-Diderot), Simon Perdrix (LORIA, CNRS, Université de Nancy), Miklos Santha (IRIF, CNRS, Université Paris-Diderot / CQT, Singapour) et Benoît Valiron (CentraleSupélec / LRI, Université Paris-Sud) offrent ici un aperçu des sujets qu'ils y ont développés. Retrouvez les vidéos de *Mathématiques en Mouvement* 2017 sur : www.sciencesmaths-paris.fr

Fondements de l'information quantique

L'ordinateur quantique est un modèle de calcul informatique inspiré de la mécanique quantique. Comme le célèbre chat de Schrödinger, à la fois mort et vivant, une particule peut, en mécanique quantique, être simultanément dans deux états, et lorsque l'on mesure un état afin de le connaître, celui-ci est perturbé irrévocablement. Que se passerait-il si on disposait de matériel informatique dont l'état serait quantique, et dont l'évolution suivrait les lois de la mécanique quantique ? Voilà l'enjeu de l'informatique quantique : identifier les tâches où un ordinateur quantique pourrait être plus performant que sa contrepartie classique. Mathématiquement, on modélise un état quantique comme un vecteur dans un espace de Hilbert. Les opérations sur les états quantiques sont représentées par des matrices unitaires. Une mesure consiste à faire une projection du vecteur modélisant l'état quantique sur l'un des vecteurs qui forment une base de l'espace considéré. Pour modéliser un calcul de façon réaliste, on se limite à un petit ensemble d'opérations de base, des *portes quantiques* qui agissent localement sur une petite portion de l'état. On construit ainsi des *circuits quantiques*. Ainsi, de la même façon que l'ordinateur traditionnel est fait de petits composants électroniques qui calculent des opérations logiques sur quelques bits à la fois, l'ordinateur quantique est composé de ces circuits quantiques. A partir de ces composants, on peut concevoir des algorithmes, des protocoles de communication, des protocoles cryptographiques, et les comparer aux meilleurs algorithmes et protocoles classiques.

Sophie Laplante

FSMP
Fondation Sciences
Mathématiques de Paris

Mathématiques en Mouvement
La prodigieuse diversité de la recherche exposée aux étudiants

L'ordinateur quantique

Conférenciers

- André Chailloux (Secret, INRIA Paris)
- Eleni Diamanti (LIP6, UPMC)
- Sophie Laplante (IRIF, Université Paris Diderot)
- Simon Perdrix (LORIA, Université de Nancy)
- Miklos Santha (IRIF, Université Paris Diderot/CQT, Singapour)
- Benoît Valiron (LRI, Université Paris Sud/CentraleSupélec)

Samedi 20 mai 2017
de 10h à 17h15
à l'Institut Henri Poincaré
11 rue Pierre et Marie Curie 75005

Inscription (obligatoire) : www.sciencesmaths-paris.fr

Logos: MATH IN NOU, DIM SIRTEQ, Recherche, SBE, casden

FONDATION SCIENCES MATHÉMATIQUES DE PARIS - WWW.SCIENCESMATHS-PARIS.FR
* IHP - 11 RUE PIERRE ET MARIE CURIE 75221 PARIS CEDEX 05
EMAIL : CONTACT@FSMP.FR - TEL : +33 1 44 27 68 03 - FAX : +33 1 44 27 68 04

Simon Perdrix

André Chailloux

