LES NOTES SCIENTIFIQUES DE L'OFFICE
OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Note n° 16 — Juillet 2019

Technologies quantiques : la programmation quantique

Source : monsitj/AdobeStock

Résumé

- *Le calcul quantique concerne aussi bien le support physique d'information (les qubits) que les langages de programmation permettant de les manipuler et d'en optimiser l'utilisation. Ces deux domaines,* a priori *distincts doivent être développés de manière synchronisée.*
- *La recherche en programmation quantique s'intéresse aussi bien au langage machine, qui contrôle les qubits, qu'à la création d'interfaces utilisateurs indépendantes de la technologie de qubits utilisée.*
- *La puissance potentielle de l'ordinateur quantique couplée à des algorithmes quantiques optimisés permettra de résoudre des problèmes à fort enjeu, tels que des calculs d'optimisation.*

M. Cédric Villani, Député, Premier vice-président

Si le succès de l'informatique repose en partie sur les progrès considérables réalisés dans le domaine de l'électronique ces dernières décennies (notamment en termes de miniaturisation conformément à la loi de Moore[1]), le développement d'algorithmes et de logiciels (traditionnellement regroupés sous le terme « *software* ») de plus en plus efficaces a également joué un rôle majeur dans son essor.

Les développeurs n'ont pas besoin de connaître le fonctionnement physique d'un ordinateur pour écrire des programmes classiques. En effet, ils utilisent le plus souvent des **langages de programmation de haut niveau**[2], orientés vers les problèmes à résoudre et qui permettent de s'affranchir des spécificités du matériel. À l'opposé, un ordinateur ne comprend que les **langages de bas niveau**, qui font faire au processeur les opérations élémentaires qu'il doit réaliser sur les bits, et dépendent donc de son architecture physique. Pour traduire efficacement les programmes de haut niveau en instructions de base, de nombreux **procédés de compilation**[3] **et d'optimisation** ont été développés dans les dernières décennies.

De la même manière, **il sera nécessaire de savoir programmer efficacement un ordinateur quantique opérationnel,** en prenant en compte ses spécificités. La programmation quantique, radicalement différente de l'informatique classique[4], commence à s'imposer comme un domaine à part entière, indispensable et complémentaire au développement de la partie matériel ou *hardware*.

Le développement de langages de programmation quantique

Contrôler des qubits et des portes logiques quantiques demande une programmation spécifique, notamment afin d'intégrer la dimension probabiliste du calcul quantique, différente du déterminisme de la physique classique. L'un des objectifs de la recherche actuelle en développement logiciel consiste à mettre au point, par anticipation, des **environnements de programmation adaptés**, qui pourront être utilisés par les programmeurs dès que des machines quantiques de capacité suffisante seront disponibles.

La création de langages de programmation quantique concerne, d'une part, des langages de bas niveau, dépendant de la technologie de qubits utilisée[5] et de ses caractéristiques (temps de cohérence, des portes logiques…[6]), d'autre part, des langages de haut niveau indépendants du système physique. Entre les deux, de nouveaux procédés de compilation doivent être développés. Plusieurs plateformes de programmation ont déjà été mises au point, certaines par des équipes académiques (comme le langage QUIPPER[7]), d'autres par des industriels qui les associent à des outils de simulation en ligne (comme le langage Q# développé par Microsoft[8]ou les langages AQASM et pyAQASM d'Atos). Des bibliothèques de calcul quantique sont également déjà disponibles en complément des langages de programmation classiques actuels comme Python. Les plateformes développées sont en général disponibles en libre accès ou dans le *cloud*, dans une perspective de recherche participative et afin de permettre au plus grand nombre de développeurs de se familiariser avec

la programmation quantique. Il importe en effet de **former rapidement des compétences de programmation suivant ces méthodes totalement nouvelles et dont la demande croît rapidement**. À cette fin, de nombreux enseignements en informatique quantique ont été mis en place autour des centres de recherche, notamment à la TU Delft (*Technische Universiteit*, Pays-Bas) ou à Télécom ParisTech.

Dans le cadre de la formation et de la recherche, l'**émulation d'ordinateurs quantiques par des machines classiques** joue également un rôle essentiel en permettant de tester des algorithmes malgré l'absence de véritable processeur quantique. Ainsi, la Q*uantum Learning Machine* (QLM), produite par Atos, est une plateforme de programmation qui simule sur un supercalculateur classique le fonctionnement d'un ordinateur quantique qui disposerait de 30 à 41 qubits. Elle permet d'intégrer les caractéristiques techniques spécifiques à chaque technologie de qubits (temps de réponses des portes logiques, décohérence…) et leur fiabilité actuelle, très utile pour des applications de bas niveau.

La recherche sur le développement de programmation quantique, quoique moins coûteuse que les développements matériels, a été très peu représentée dans les financements de la première phase du *flagship* européen sur les technologies quantiques lancée en octobre 2018[9]. **Des efforts d'investissement doivent pourtant être menés dans ce domaine afin d'anticiper l'utilisation de machines quantiques et leur mise en application.** En France, le projet ANR SoftQPro[10], financé à hauteur de 500 000 € jusqu'en 2022, regroupe le CEA, Atos et plusieurs laboratoires universitaires d'informatique afin de développer des méthodes d'optimisation de programmes quantiques.

Algorithmes quantiques et applications

Seulement une soixantaine de classes d'algorithmes quantiques ont été développées à ce jour, la recherche étant assez récente.

Ils permettent, en théorie, de résoudre certains problèmes plus efficacement qu'une machine classique, par exemple en arithmétique (factorisation de grands nombres[11], *cf. encadré*) ou pour les problèmes d'optimisation, qui cherchent le minimum et/ou le maximum d'une quantité donnée. La palette des secteurs concernés par les problèmes d'optimisation est extrêmement large, allant de la santé et de la chimie (configuration de molécules) à la finance (optimisation de portefeuilles) en passant par la logistique et la gestion de ressources.

La différence entre algorithme classique et quantique : l'exemple de l'algorithme de Shor

La factorisation de grands nombres entiers constitue la base des méthodes de chiffrement actuelles, notamment via le protocole RSA(*), utilisé depuis les années 1970. En effet, ce problème s'avère particulièrement difficile à résoudre pour un ordinateur classique. Dès 1994, Peter Shor, chercheur américain, écrit un algorithme qui, s'il existait un ordinateur quantique susceptible de le mettre en œuvre, permettrait de factoriser des nombres entiers en un temps exponentiellement plus rapide que les algorithmes classiques connus, et donc, deviendrait une menace pour la sécurité des protocoles de chiffrement utilisés.

Le principe de la résolution d'un problème de factorisation consiste à le transformer en un problème de recherche de période (ou de fréquence, qui est l'inverse de la période). Une manière de se représenter ce concept est d'imaginer un livre qui, d'une part, contiendrait beaucoup de pages et d'autre part, serait périodique : il serait en fait composé d'une même histoire qui se répète toutes les n pages (n étant la période)(**).

La méthode classique consiste à passer en revue toutes les pages depuis le début jusqu'à en trouver deux identiques. Comme le livre est très gros, cette méthode demande beaucoup de temps et de mémoire.

Le paradigme de l'algorithme quantique de Shor est totalement différent : dans un premier temps, le principe de superposition permet à des qubits de représenter toutes les pages du livre en même temps ; grâce à une « transformation de Fourier », méthode mathématique utilisée dans de nombreux domaines de la physique et permettant de décomposer un signal en fonction d'une variable indépendante qui peut s'interpréter en physique comme sa fréquence ou sa pulsation, il s'agit ensuite d'identifier et d'amplifier la fréquence (ou période) la plus probable pour la mesurer. Ainsi, avec la méthode quantique, il n'est pas nécessaire de connaitre le contenu précis du livre, ce qui rend le calcul beaucoup plus rapide.

(*) Voir la note de l'Office : « Les technologies quantiques : la cryptographie quantique et post-quantique »

(**) Analogie inspirée de l'article: https://www.larecherche.fr/traquer-les-failles-des-algorithmes

En particulier, se trouvent les problèmes dits **NP-complets**[12], pour lesquels on ne connaît pas de méthode de résolution plus efficace que le test de toutes les possibilités, mais dont la vérification d'une solution proposée est rapide. Pour ces problèmes, les temps d'exécution des algorithmes de résolution varient exponentiellement avec la taille des données d'entrée et nécessitent des temps d'exécution très longs sur des machines classiques. Les algorithmes « quantiques » permettraient de les réduire considérablement. **L'énoncé dit du « voyageur de commerce » constitue un des exemples les plus connus de cette classe de problèmes** et vise à calculer quel est le trajet le plus court pour un voyageur de commerce lors de sa mission, en sachant que celui-ci doit passer dans chaque ville dont il est chargé, mais une et une seule fois[13].

L'alliance entre des processeurs classiques et quantiques serait idéale pour optimiser le temps de calcul de ce type de problème, les qubits pouvant explorer efficacement chaque piste de solution possible, que les bits classiques vérifieraient rapidement. **Ceci constitue un bon exemple du potentiel de complémentarité entre les deux technologies.** Une réflexion est également en cours sur l'alliance possible du potentiel de calcul quantique avec les techniques de *deep learning*[14].

Si ces applications semblent prometteuses, **les machines quantiques actuelles, trop limitées et trop peu fiables, ne permettent pas encore de réaliser des calculs qui soient aujourd'hui inaccessibles aux (super) calculateurs classiques et d'explorer complètement le champ des possibilités quantiques**. Les tests s'effectuent encore sur un nombre très restreint de qubits mais permettent de valider des schémas d'algorithmes et des pistes de recherche. Une mise en évidence expérimentale de la supériorité du calcul quantique, appelée « **suprématie quantique**[15] », nécessiterait de disposer d'au moins une centaine de qubits, et constitue un enjeu majeur pour lancer un cycle vertueux de recherche et de commercialisation.

Conclusion et recommandations

Les domaines de la programmation et de l'algorithmie quantiques ne doivent pas être négligés, notamment afin de déployer pleinement le potentiel de l'informatique quantique et de répondre à des applications spécifiques, comme des calculs d'optimisation qui trouvent de nombreuses applications. Même s'il est difficile de prévoir à quelle échéance un ordinateur quantique disposant de plusieurs centaines, voire milliers, de qubits sera disponible, il reste nécessaire d'anticiper son arrivée, *via* l'utilisation d'émulateurs quantiques par exemple. Cette méthode pourra aussi permettre la mise en évidence, par sérendipité, de nouveaux problèmes inaccessibles aux processeurs classiques mais à la portée de registres de qubits.

Internet de l'OPECST :
http://www.assemblee-nationale.fr/commissions/opecst-index.asp
http://www.senat.fr/opecst/

Personnes auditionnées

M. Alain Aspect, physicien à l'Institut d'Optique, membre du Conseil scientifique de l'Office.

Mme Astrid Lambrecht, directrice de recherche au CNRS, directrice de l'Institut de physique du CNRS (INP/CNRS), membre du conseil scientifique de l'Office.

Mme Fanny Bouton, journaliste spécialisée dans les nouvelles technologies.

M. Antoine Browaeys, directeur de recherche à l'Institut d'Optique.

M. Philippe Chomaz, directeur scientifique exécutif de la Direction de la recherche fondamentale au CEA.

M. Bruno Desruelle, PDG de la start-up Muquans.

M. Philippe Duluc, directeur technique big data & security d'Atos.

M. Daniel Estève, directeur de recherche et chef du groupe Quantronique au CEA.

M. Olivier Ezratty, consultant spécialisé en nouvelles technologies et auteur du blog "Opinion libres".

M. Philippe Grangier, Directeur de Recherche CNRS et Responsable du Groupe Optique Quantique à l'Institut d'Optique.

M. Serge Haroche, professeur émérite au Collège de France, prix Nobel de physique 2012.

M. Christophe Jurczak, directeur général du fonds d'investissement Quantonation.

M. Iordanis Kerenidis, directeur de recherche CNRS à l'Institut de recherche en informatique fondamentale (IRIF).

Mme Pascale Senellart, directrice de recherche au Laboratoire de photonique et nanostructures (LPN) du CNRS. Co-fondatrice de la start-up Quandela.

M. Miklos Santhas, directeur de recherche au Laboratoire d'Informatique Algorithmique : Fondements et Applications (LIAFA).

M. Sébastien Tanzilli, Directeur de recherche et chargé de mission au CNRS sur les technologies quantiques.

M. Georges Uzbelger, AI/Advanced Analytics Solution chez IBM France.

M. Benoit Valiron, Professeur assistant à Centrale Supélec.

M. Benoit Wintrebert, Conseiller en Innovation au Ministère des Armées.

Coordination scientifique de Mme Sarah Tigrine, conseillère scientifique (avec la participation de M. Gaëtan Douéneau).

Ouvrages de référence consultés :

- « Comprendre l'informatique quantique » O. Ezratty, novembre 2018 (e-book)

- Rapport des Académies américaines : National Academies of Sciences, Engineering, and Medicine. 2018. Quantum Computing : Progress and Prospects. The National Academies Press, Washington, DC. DOI : https ://doi.org/10.17226/25196.

- « Clefs du CEA » N° 66- juin 2018 « révolutions quantiques »

Nota : en accord avec la déontologue de l'Assemblée nationale, Cédric Villani s'est mis en retrait de sa participation au Conseil scientifique d'ATOS – organe non décisionnel – pour la durée de ses travaux pour l'Office portant sur les technologies quantiques.

Références

(1) En 1965, Gordon E. Moore (un des trois fondateurs d'Intel) énonçait ce que nous appelons maintenant la loi de Moore, à savoir que la densité des transistors (nombre de transistors par unité de surface) – dont découle la puissance de calcul des ordinateurs classiques - pourrait doubler tous les deux ans. Cette prédiction s'est révélée étonnamment exacte, et ces dernières années, les finesses de gravure n'ont cessé de diminuer jusqu'à atteindre 10 nm, (1 nm=10^{-9} m) en 2017. Cependant, ces progrès atteignent des limites physiques du fait que l'on approche les dimensions de l'atome.

(2) La notion de « haut niveau » s'entend du niveau de la machine, par opposition au langage de « bas niveau » qui correspond aux instructions données au processeur de la machine.

(3) En informatique, la compilation désigne la traduction du code de haut niveau, écrit par l'utilisateur, en instructions d'un langage de bas niveau, compréhensible par la machine. Un compilateur optimisé permet, par exemple, d'augmenter la vitesse d'exécution des instructions ou de réduire l'espace mémoire occupé.

(4) En effet, les principes de la physique quantique imposent des contraintes sur les bits quantiques, par exemple l'impossibilité de recopier une valeur.

(5) Plusieurs technologies de qubits sont actuellement à l'étude, comme les ions piégés, les atomes froids, les qubits de spin ou les qubits supraconducteurs. Voir à ce sujet la note « Technologies quantiques : l'ordinateur quantique » de l'Office.

(6) Cf. la note « Technologies quantiques : l'ordinateur quantique » de l'Office.

(7) https://www.mathstat.dal.ca/~selinger/quipper/

(8) https://www.lemondeinformatique.fr/actualites/lire-microsoft-pousse-sur-github-une-formation-au-developpement-quantique-72407.html

(9) http://www.cnrs.fr/fr/premiers-laureats-pour-linitiative-europeenne-sur-les-technologies-quantiques

(10) https://anr.fr/Projet-ANR-17-CE25-0009

(11) Voir la note de l'Office « Technologies quantiques : cryptographies quantique et post-quantique ».

(12) Il existe des milliers de problèmes dits NP complets dont le problème du sac à dos, le problème de la plus longue chaîne…

(13) Des applications directes du problème du voyageur de commerce concernent, par exemple, la logistique et les systèmes de livraison ; mais des applications moins évidentes ont été mises en évidence, comme l'optimisation du mouvement d'une machine industrielle, par exemple la réduction du temps mis par une perceuse électronique pour percer un nombre donné de trous.

(14) https://www.nature.com/articles/d41586-019-00771-0 pour une analyse de l'étude Havlíček, V. et al. Nature 567, 209–212 (2019).

(15) Plusieurs expressions visent à comparer les performances d'un ordinateur quantique et d'un supercalculateur classique : l'expression « avantage quantique » désigne le cas où un problème est traité avec une méthode quantique plus rapidement qu'avec un supercalculateur ; la « suprématie quantique » correspond à la situation dans laquelle la technologie quantique permettrait de réaliser des traitements inaccessibles aux ordinateurs classiques.