Révolution quantique (2/5): l'ordinateur surpuissant est en vue

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE LUNDI 1 AOÛT 2016

Les principes de la physique quantique ont ouvert, en matière d'informatique, de nouvelles perspectives qui devraient bouleverser le monde du numérique : l'ordinateur quantique permettra, à terme, de révolutionner de nombreux domaines comme l'intelligence artificielle ou le chiffrement.

Imaginez un ordinateur si puissant qu'il serait capable de simuler l'ensemble de l'univers, l'intégralité de ses processus physiques depuis le big-bang. De la science-fiction ? Pas totalement. Dans son livre publié en 2006, *Programmer l'univers*, Seth Lloyd, chercheur au MIT (Massachusetts Institute of Technology) et spécialiste de la physique quantique, avance même **une thèse bien plus audacieuse** : l'univers lui-même ne serait qu'un immense ordinateur quantique au sein duquel nous vivrions.

Et cette affirmation n'est pas faite sans base scientifique. Avant Seth Lloyd, le physicien britannique David Deutsch, pionnier de la physique quantique, avait repris une thèse formulée dans les années 1930 pour l'informatique classique par les mathématiciens Alonzo Church et Alan Turing. Formulée en 1985, cette nouvelle thèse baptisée **« principe Church-Turing-Deutsch »**, ou « principe CTD », fait le pari qu'un ordinateur quantique sera capable de simuler tout processus physique.

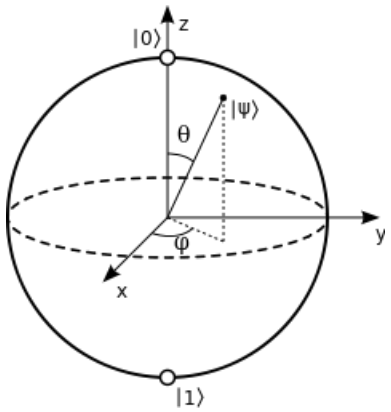
Mais qu'est-ce qu'un ordinateur quantique ? Le sujet est particulièrement à la mode et une explication concise a été donnée par le premier ministre canadien Justin Trudeau lors d'une intervention très médiatisée à l'institut Périmètre de Waterloo, un centre de recherche étudiant les théories de la physique.

En résumé, et sans revenir sur les principes de la physique quantique **expliqués précédemment**, il s'agit d'un ordinateur n'utilisant plus de « bits » gravés sur des puces informatiques mais des « qubits », des informations dont les supports sont désormais des particules, atomes, électrons ou encore photons. En informatique classique, un bit est une unité ne pouvant prendre que deux valeurs, le 0 ou le 1, servant à encoder les informations.

L'informatique quantique, elle, prend comme supports des particules et utilise les propriétés de la physique quantique, à commencer par **la superposition d'états**. Dans le monde quantique, il faut réussir à accepter que rien n'est déterminé. Un objet est en effet décrit comme ayant tous les états possibles, en termes de position, de vitesse, etc. Ce n'est que lorsqu'on le mesure qu'il prend des valeurs fixes. En 1935, le physicien autrichien Erwin Schrödinger avait imaginé une expérience de pensée afin de mieux appréhender ce monde qui défie notre logique, restée célèbre sous le nom de l'expérience du **« chat de Schrödinger »**. Imaginez un chat enfermé dans une boîte avec une capsule de poison reliée à un corps radioactif. Dès qu'un de ses atomes se fissure, la capsule de poison est brisée et le chat meurt. Pour déterminer l'état du chat enfermé dans la boîte, la logique voudrait calculer les probabilités pour que l'atome se fissure. Mais la physique quantique, elle, raisonne autrement : le chat est à la fois mort ET vivant. Il ne sera l'un ou l'autre que lorsqu'on ouvrira la boîte.

Une fois acceptée la logique quantique, il suffit de l'appliquer à des atomes ou des photons pour graver des informations. Les qubits ne sont ainsi pas limités par le choix entre 0 et 1 et possèdent plusieurs valeurs en même temps. La puissance des ordinateurs quantiques est donc, en théorie, démultipliée par rapport aux ordinateurs classiques. Reposant sur des principes de calcul totalement différents de

l'informatique classique, ils permettront en outre de faire tourner des algorithmes quantiques réalisant des opérations jusqu'à présent inaccessibles.



La représentation d'un qubit © Wikipedia

Mais les principes de la physique quantique, dont l'un affirme que ses règles disparaissent à l'échelle macroscopique, imposent ainsi des contraintes matérielles très fortes. Le support du qubit doit non seulement être une particule, atome ou photon, mais en plus être conservé dans des conditions d'isolation extrêmes. Ces contraintes physiques limitent actuellement fortement le développement des ordinateurs quantiques.

En réalité, lorsque l'on parle aujourd'hui d'ordinateur quantique, il faut distinguer deux systèmes. Le premier est l'ordinateur « réellement » quantique, appelé ordinateur quantique universel, fonctionnant entièrement de manière quantique. Celui-ci n'en est encore qu'à ses balbutiements et il n'en existe à ce jour aucune version pleinement fonctionnelle. En revanche, plusieurs laboratoires ont développé des ordinateurs partiellement quantiques, appelés ordinateurs « adiabatiques », déjà en activité. Ces machines utilisent un dispositif quantique, mais de manière limitée.

« Les ordinateurs quantiques adiabatiques sont plus faciles à fabriquer, ils comportent plus de qubits mais ils ne permettent pas de traiter les algorithmes quantiques et ne peuvent résoudre que des fonctions d'optimisation bien précises, explique Renaud Lifchitz, expert en sécurité chez Digital Security. *Ces ordinateurs sont typiquement utilisés par des industriels ou de grandes entreprises pour calculer le frottement d'une carlingue avec l'air, ou pour optimiser en Bourse un portefeuille d'actions en fonction des variations du marché. L'ordinateur quantique adiabatique le plus connu est celui de* ***la société canadienne D-Wave****, qui a maintenant déjà connu plusieurs générations. Équipé de 2 048 qubits, il est pour l'instant réservé à quelques grands groupes comme Google, Lockheed-Martin ou encore la Nasa. Ces machines sont très chères et elles nécessitent, pour fonctionner, des équipes de physiciens et d'informaticiens ainsi que des infrastructures très lourdes. Concernant leur efficacité, il y a toujours des débats techniques sur le régime quantique ou non des opérations effectuées. Mais on peut estimer que D-Wave les effectue plusieurs milliers de fois plus rapidement qu'un ordinateur classique. Une autre application des ordinateurs adiabatiques est le* deep learning [**apprentissage profond** en français : désigne les méthodes informatiques d'apprentissage automatique ; **le programme AlphaGo**, connu pour avoir battu le champion du monde de jeu de go en mars dernier, reposait sur le *deep learning* – ndlr]. *C'est déjà utilisé par Google, notamment dans le cadre de plusieurs projets comme leur projet de voiture intelligente. »*

Les ordinateurs quantiques universels, eux, sont encore loin d'être utilisables en pratique, même si plusieurs projets sont bien avancés. L'université de Bristol par exemple a réussi en 2010 à faire tourner un algorithme quantique sur une de ses machines. *« L'ordinateur de l'université de Bristol est universel, mais il serait plus juste de parler d'une puce, assez limitée même si elle est très complexe,* explique Renaud Lifchitz. *Elle est limitée à 2 qubits. Il n'en reste pas moins qu'il s'agit d'un système industriel qui fonctionne. C'est une véritable prouesse. IBM de son côté propose une puce universelle de 5 qubits, mais également avec des limitations. En laboratoire, des chercheurs ont réussi à aller jusqu'à 12 qubits avec pas mal d'efforts. Grâce à ceux-ci, on a réussi à montrer que des algorithmes quantiques conçus il y a des années, comme l'algorithme de Shor, tournaient très bien. »*

Les algorithmes quantiques

Car c'est l'un des grands enjeux de l'informatique quantique : la possibilité de réaliser des opérations jusqu'à présent impossibles à calculer. Les machines quantiques universelles permettront notamment de s'attaquer à la cryptographie d'une manière inédite. Plus précisément, deux algorithmes quantiques déjà existants suscitent des inquiétudes. L'un vise le chiffrement dit symétrique, c'est-à-dire reposant sur une seule clef de chiffrement, utilisé par exemple dans la sécurisation de visites de sites internet. L'autre vise le chiffrement dit asymétrique, c'est-à-dire reposant sur un échange de clefs de chiffrement entre deux personnes, utilisé pour sécuriser les communications.

« Concernant la cryptographie symétrique, c'est l'algorithme de Grover qui s'applique. Celui-ci permet, en résumé, de diviser par deux la taille de toutes les clefs utilisées, détaille Renaud Lifchitz. *Par exemple, une clef AES de 128 bits face à l'algorithme n'aura la résistance que d'une clef AES de 64 bits. Les clefs seront simplement deux fois plus faciles à casser. Or, on sait déjà que l'algorithme de Grover est optimal. Pour la cryptographie symétrique, nous avons donc une solution simple : il suffira de doubler la taille de toutes les clefs pour rester hors de portée d'attaques quantiques. »*

«Concernant la cryptographie asymétrique, c'est un peu plus compliqué, poursuit Renaud Lifchitz. *Là, c'est l'algorithme de Shor, qui permet notamment de casser les échanges de clefs, qui s'applique. Le problème est que l'algorithme de Shor est* ***polynomial****. Doubler la taille des clefs ne sera donc pas suffisant : l'attaquant n'aura besoin que d'un peu plus de temps pour réussir. Ici, la seule solution est de réfléchir à une autre cryptographie car, si on ne peut plus avoir confiance dans le cryptage, on ne peut plus avoir confiance en rien. Depuis plusieurs années, la conférence PQCrypto (pour* ***Post Quantum Crypto)*** *tente d'imaginer la crypto de demain. »* De son côté, le géant américain **Google vient d'annoncer** qu'il avait implémenté dans ses serveurs un algorithme « post-quantique » censé protéger les utilisateurs de son navigateur Chrome des futures attaques quantiques.

Mais l'informatique quantique a aussi des applications en matière de sécurité, comme **la distribution de clefs quantiques**, une technologie développée notamment en Suisse dès 2008 avec **le projet SwissQuantum** de l'université de Genève. *« Cela nécessite deux canaux, un pour envoyer le message chiffré, et un autre, constitué de fibre optique, pour échanger la clef qui permettra de déchiffrer le message*, explique Renaud Lifchitz. *Il existe une loi, dans* ***la théorie de l'information de Shannon****, qui stipule que si la clef est aussi longue que le message, celui-ci est incassable. Le but, ici, est donc de protéger la clef qui est envoyée par fibre optique. Or, en physique quantique, lorsque l'on observe une particule, on la modifie. Donc, si un attaquant essaye d'intercepter la clef, il la modifie et la détruit. L'autre avantage de ce système est que l'on sait, à la réception, si quelqu'un a essayé d'intercepter les clefs car le seul fait de l'observer la modifie. Et en plus, l'attaquant sait tout cela. C'est donc en quelque sorte le système parfait en termes de sécurité. Par contre, il ne peut fonctionner que de pair à pair, entre deux points. De plus, pour conserver les propriétés quantiques, le canal de fibre optique ne peut dépasser une centaine de kilomètres. Mais il est déjà utilisé pour les transactions financières en Suisse où les établissements bancaires sont assez proches les uns des autres. Et des sociétés commercialisent des routeurs quantiques. »*

Quand ces machines quantiques seront-elles disponibles pour le grand public et que changeront-elles dans notre vie quotidienne ? *«Avant tout, il faudra que ces ordinateurs fonctionnent avec un très grand nombre de qubits et une isolation extrême. Ensuite, il*

faudra qu'ils aient une taille suffisante pour trouver une application civile intéressante », résume Renaud Lifchitz.

Un ordinateur quantique de la société D-Wave © Reuters

« Il est très difficile de faire des prédictions, mais jusqu'à présent, il semblerait que les ordinateurs quantiques suivent eux aussi ***la loi de Moore***[qui stipule que la capacité des ordinateurs double tous les 18 mois – ndlr]. *Si les progrès continuent à ce rythme, je pense qu'on peut espérer un ordinateur quantique universel mature d'ici à 20-25 ans. Après, il n'y a pas vraiment de limite. Les changements ne seront pas forcément visibles, mais les principaux protocoles de l'Internet devront être changés. Les principales avancées se feront probablement sentir dans le domaine des interfaces homme-machine, dans l'intelligence artificielle, ou encore l'analyse de texte. Par exemple, aujourd'hui, pour un moteur de recherche, nous avons beaucoup de mal à traiter une requête du type "je veux partir en voyage dans un endroit où il fait chaud, en Europe, pas trop loin de la mer, et où il fait entre 25 et 30 degrés aux mois d'août et septembre". Ce type de demande peut être traité par la recherche sémantique. Tout ce qui a trait au* machine learning [l'auto-apprentissage des machines et des intelligences artificielles – ndlr] *va également connaître un bond. »*

Il ne faudra cependant pas espérer disposer de son propre ordinateur quantique à domicile. *« Je ne pense pas que l'individu lambda aura son propre ordinateur quantique universel personnel à court ou moyen terme,* estime Renaud Lifchitz. *Tout d'abord parce que c'est très cher. Il faut assurer une isolation totale de l'ordinateur, qu'il n'y ait aucun échange de gaz ou de lumière ainsi qu'un refroidissement extrême. Des conditions qui ne sont pas envisageables pour des particuliers. Ensuite parce que ces ordinateurs seront certainement utilisés uniquement pour faire tourner des algorithmes quantiques. En effet, il n'y a aucun intérêt à faire tourner des algorithmes classiques sur un ordinateur quantique qui n'est pas fait pour ça et qui est plus lent qu'un ordinateur classique dans ce cas. Selon moi, les ordinateurs quantiques seront principalement accessibles via le Cloud, où l'on louera du temps de calcul. »*

Au mois de juin dernier, le cofondateur du système d'exploitation Android, racheté depuis par Google, Andy Rubin avait également donné **sa version de notre futur quantique** lors d'une conférence organisée à San Francisco. À cette occasion, cet ingénieur et programmeur, reconverti en *business angel*, a révélé avoir investi dans une entreprise qui s'est donné pour but de commercialiser des appareils quantiques. Comme Renaud Lifchitz, Andy Rubin estime que l'avenir de l'informatique quantique n'est pas tant dans les machines que dans la relation homme-machine, et plus particulièrement dans l'intelligence artificielle (IA). Les algorithmes quantiques permettront en effet de développer de formidables IA, tellement puissantes qu'une seule suffirait à gérer tous vos appareils électroniques. *« Si vous avez une informatique aussi puissante que ce qu'elle pourrait être, vous pourriez n'en avoir besoin que d'une,* a notamment déclaré Andy Rubin. *Ça ne serait pas quelque chose que vous transporteriez avec vous ; elle n'aurait qu'à être consciente. »* Cette intelligence artificielle *« consciente »* aurait bien entendu besoin d'une énorme quantité de données. *« C'est là que la robotique entre en jeu »*, poursuit Andy Rubin qui imagine un monde où nous serions tous équipés d'une multitude de capteurs alimentant notre IA quantique.

Quant à simuler l'univers, Renaud Lifchitz est tout aussi sceptique. *« On ne sait déjà pas simuler le cerveau humain. Un premier pas serait déjà de simuler de petits systèmes,* explique-t-il. *Mais surtout, se posent des questions fondamentales et presque philosophiques: notre cerveau a-t-il un fonctionnement quantique ? Tout est-il régi par les lois de la physique quantique ? Si je prends un médicament par exemple, a-t-il un effet quantique ? Si la réponse est oui, se pose alors un autre problème. L'un des principes de la physique quantique est* ***celui de non-***

clonage [qui interdit le clonage d'un état quantique – ndlr]. *On ne peut pas cloner une particule. Donc, si le cerveau a un fonctionnement quantique, on ne pourra ni le cloner ni le simuler. »*

« Les problématiques sont les mêmes au niveau de l'univers, poursuit Renaud Lifchitz. *On ne sait pas s'il a un fonctionnement quantique et, si c'est le cas, il est impossible de cloner l'état quantique d'un système. En résumé, si l'on veut simuler, il ne faut pas que ce soit quantique. Le principe* ***Church-Turing-Deutsch*** *fonctionne, mais dans le cadre de la physique classique. On sait qu'il y a environ 10 puissance 90 particules dans l'univers. Et techniquement, pour représenter tout ça, il suffit de 300 qubits, ce qui devrait arriver d'ici à une vingtaine d'années. À cette date, nous ne serons peut-être pas capables de le simuler, mais nous pourrons énumérer tous les atomes de l'univers un par un. Ça serait déjà pas mal ! »*

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.