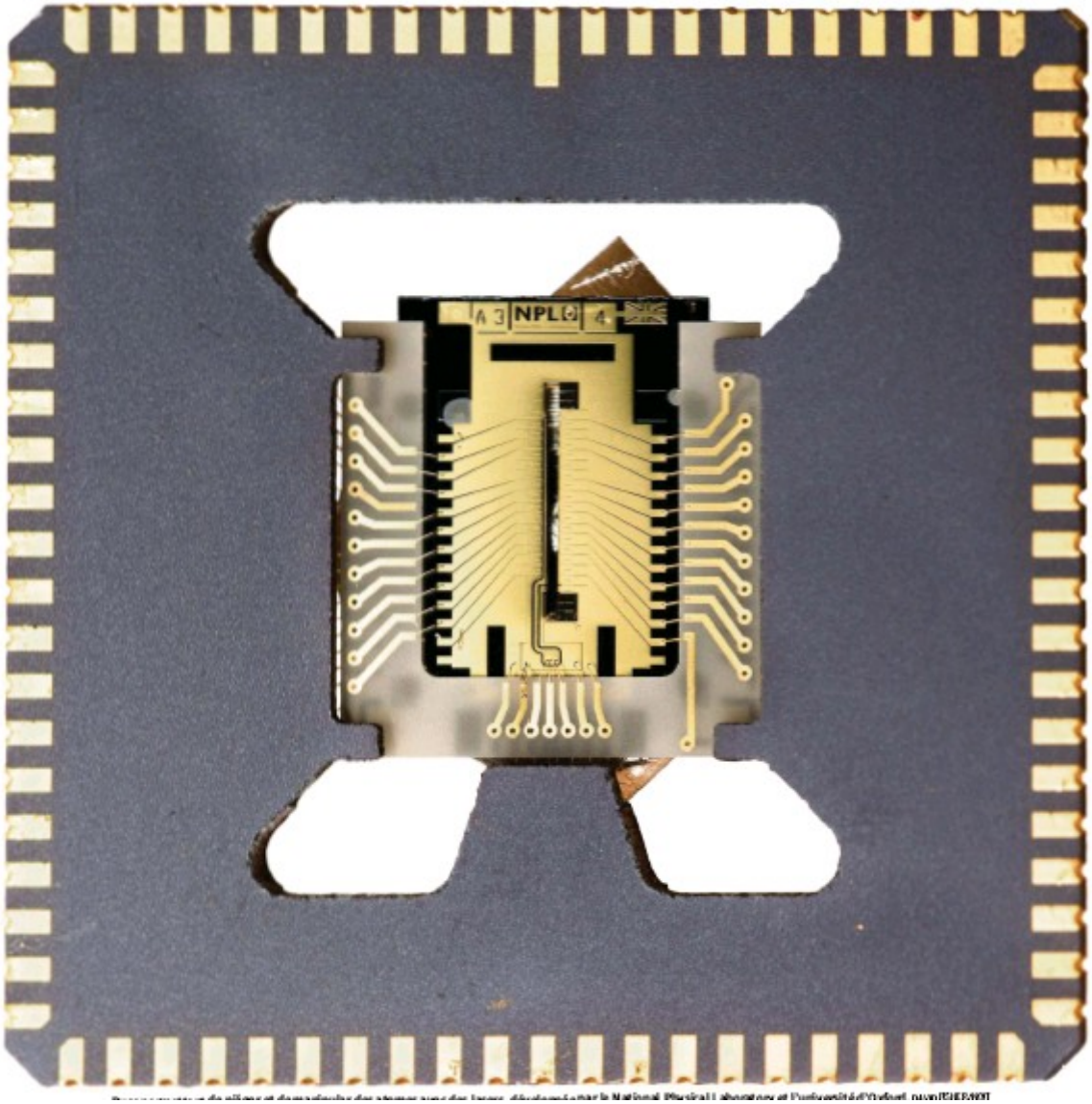
# L'ORDINATEUR QUANTIQUE RÉVOLUTIONNE L'INFORMATIQUE

Depuis que les géants du numérique sont entrés dans la course, le développement des ordinateurs à base de « qubits » a pris un coup d'accélérateur. Ces machines, qui font appel aux propriétés déroutantes de la matière, offrent des capacités de calcul inéd

Le Monde · 5 Jul 2017 · david larousserie delft (pays-bas) - envoyé spécial

C'est du sérieux!», s'enthousiasme Lieven Vandersypen, du laboratoire QuTech à l'université de Delft (Pays-Bas), en brandissant un gros disque de la taille d'un 33-tours. C'est une plaquette de silicium, fabriquée par Intel, qui ressemble à celle des microprocesseurs, gravée de milliards de transistors, qui dopent nos ordinateurs et autres mobiles. Sauf qu'elle contient les premières briques de ce qui pourrait constituer le coeur d'une machine d'un nouveau genre: un ordinateur quantique. Ce concept, imaginé dans les années 1980, est longtemps resté une arlésienne, comparable à la fusion nucléaire dans le domaine de l'énergie. Autrement dit, une approche révolutionnaire, promettant de battre les meilleurs supercalculateurs actuels, mais faisant face à de sérieux obstacles pour sa réalisation concrète. Elle tire profit de la théorie quantique, qui décrit la matière au niveau atomique, et surtout de ses propriétés radicalement différentes de la physique classique.



«La donne concernant l'informatique quantique est en train de changer, constate Leo Dicarlo, également à QuTech. Le moment devient plus excitant avec l'implication des industriels. » Ces derniers mois lui donnent raison. Les géants Google, IBM, Microsoft ou encore Intel ont annoncé plusieurs percées dans le domaine. Depuis le printemps, n'importe qui peut se connecter à un service d'IBM donnant accès à un ordinateur quantique, doté de trois fois plus de composants que celui mis à disposition en 2016. Une version améliorée de cette machine peut même être achetée pour ceux qui ne voudraient pas partager leurs calculs.

→

«Même si cela reste de la R&D, nous avons progressé et avons confiance: dans la prochaine décennie un ordinateur quantique universel sera développé, indique Xavier Vasques, directeur technique chez IBM France. L'ouverture de ce système permet d'explorer les collaborations et de créer un écosystème pour accélérer son adoption. » Près de 300000 expériences quantiques ont déjà tourné sur ces ordinateurs pour 40 000 utilisateurs, communique IBM.

Google revendique, lui, depuis mai, d'avoir fabriqué le plus gros de ces ordinateurs nouvelle génération. Il est environ un tiers plus gros que celui d'IBM, et son successeur, attendu dans les prochains mois, sera deux fois plus performant. Il pourrait être le premier à montrer la suprématie du quantique sur le monde du calcul classique. Ces progrès sont notamment dus au recrutement en 2014 d'une des vedettes académiques du domaine, John Martinis, de l'université de Californie, à Santa Barbara.

Chez Microsoft ou chez le français Atos, des machines classiques, capables de simuler le comportement des ordinateurs quantiques, sont désormais en vente. Là encore, pour préparer le monde à la révolution annoncée.

QuTech même est le symbole du nouveau souffle quantique. Le laboratoire a été lancé en 2014, à partir d'une équipe de recherche fondamentale de l'université de Delft. En 2015, il reçoit le label «icône nationale» et plus de 135millions de dollars (119millions d'euros) sur dix ans. Leo Kouwenhoven, le fondateur, a depuis été recruté par Microsoft, qui ouvre un site sur le campus pour ses propres activités et des collaborations avec QuTech.

«Les entreprises partenaires, comme Intel ou Microsoft, ont été impressionnées par nos divers atouts en science, en ingénierie, en théorie… Ils nous ont dit ne pas avoir trouvé une telle concentration ailleurs, y compris aux Etats-Unis », explique Kemo Agovic, le directeur administratif de ce laboratoire. «Ce n'est plus de la pure physique quantique, mais déjà de l'ingénierie en électronique, en informatique, en optique, en logiciels…», estime Garrelt Alberts, de l'Institut néerlandais de recherche appliquée (TNO), partenaire de QuTech, devenu le plus gros laboratoire d'Europe dans le domaine.

La cinquantaine de chercheurs du départ a déjà presque triplé et pourrait atteindre 250 d'ici à 2020. En 2016, c'est de ce campus qu'est partie l'initiative européenne destinée à financer, à hauteur de 1milliard d'euros sur dix ans, des activités autour de l'information quantique. Les premiers appels d'offres sont attendus pour 2018.

A l'intérieur, l'aménagement ressemble plus à celui d'une start-up qu'à celui d'une université. Les bureaux sont en open space. Les expériences nécessitent des systèmes de refroidissement à l'hélium liquide, assez bruyants, qui sont regroupés sur un étage, séparé des ordinateurs permettant de les contrôler, pour plus de tranquillité. Le nombre de ces frigos dépasse la trentaine, deux fois plus qu'en 2014. C'est en leur sein que battent les futurs coeurs des ordinateurs quantiques.

Ils n'ont plus rien à voir avec les transistors et processeurs actuels. Dans ces derniers, l'information est codée avec des 0 et des 1 (les bits d'information) et traitées par des transistors, sorte d'interrupteurs à courant électrique. L'assemblage de plusieurs de ces transistors permet de trier les bits, de les ajouter, de les retrancher…

Mais alors qu'un interrupteur est soit ouvert (codant pour 1), soit fermé (codant pour 0), son équivalent quantique peut être ouvert et fermé à la fois, et donc valoir 0 et 1 dans le même temps. Ce qubit, pour bit quantique, est techniquement une superposition de 0 et 1, une sorte de mélange des deux. Comme un peintre qui passerait du noir et blanc au niveau de gris, voire à la couleur, l'ingénieur peut alors faire déborder son imagination.

Contrôler sans détruire

Quantitativement, le gain est énorme. Un qubit peut encoder deux bits; deux qubits peuvent encoder quatre bits, ou plus généralement N qubits équivalent à 2N bits. Petit détail qui complique néanmoins les choses: si mesurer un bit ne change pas sa valeur, mesurer un qubit le fait se précipiter avec une certaine probabilité soit vers la valeur 0, soit vers la valeur 1. Tel le carrosse se transformant en citrouille, la magie est rompue. Tout l'art des ingénieurs consiste donc à contrôler ces qubits, sans les détruire.

En outre, la superposition et cette capacité à être dans deux états à la fois n'est pas la seule bizarrerie quantique profitable pour les calculs. Il y a aussi l'intrication, c'est-à-dire l'art d'assembler deux qubits – ou plus –- de manière à ce qu'il ne fasse qu'un. Ces deux propriétés confèrent une sorte de parallélisme intrinsèque à l'ordinateur quantique et apportent de la liberté aux concepteurs de pro-

grammes, afin de faire mieux que des équivalents classiques. En 1994 et 1996, deux algorithmes ont ainsi été proposés, dont l'efficacité est supérieure aux ordinateurs classiques. L'un permet de rechercher un mot dans un dictionnaire. L'autre trouve les diviseurs d'un entier. Plus le dictionnaire est gros ou plus l'entier est gros, plus les calculs sont longs, mais le protocole quantique demande moins de temps que son homologue classique.

La recherche s'adapte aussi aux modes actuelles, comme l'apprentissage machine, une technique très à la mode d'intelligence artificielle. En mars 2017, Ioardanis Kerenidis, directeur de recherche CNRS à l'Institut de recherche en informatique fondamentale (université ParisDiderot), a ainsi présenté un algorithme de recommandation de films, de livres ou de rencontres, « exponentiellement plus efficace que les méthodes actuelles ».

Reste à fabriquer ces fameux qubits. Les idées et réalisations foisonnent, avec chacune leurs avantages et leurs inconvénients. Leur point commun est d'utiliser des objets capables d'être dans deux états à la fois, souvent équivalents à l'aiguille d'une boussole pointant vers le haut, le bas (l'équivalent des 0 et 1 classiques) ou toute position intermédiaire. A partir de là, le choix est grand : atomes, électrons, photons… qui « tournent » avec des lasers, des micro-ondes, des tensions électriques. « Toutes ces bizarreries quantiques, superposition, intrication… sont devenues pour nous du quotidien», résume Leo Dicarlo.

Un des dispositifs les plus populaires chez les industriels est un circuit électronique dans lequel les charges peuvent être à deux endroits à la fois. Il est plutôt simple à fabriquer, et surtout à répliquer et multiplier. C'est l'option choisie par IBM et Google pour leurs machines de respectivement 17 et 22 qubits.

Alors, à quand la défaite du plus gros supercalculateur actuel, le chinois Sunway TaihuLight? Pas tout de suite, car un obstacle subsiste. « Tout pousse un système quantique à devenir classique », résume Adrien Facon, de l'entreprise de sécurité informatique Secure-IC, chargé de réfléchir aux parades à élaborer face aux attaques quantiques.

Autrement dit, la magie quantique des qubits a tendance à disparaître avec le temps, à cause des interactions avec l'extérieur ou à force d'être manipulés. Et les précieux avantages sont perdus. « Nous avons progressé. En 2005, nos qubits, des électrons confinés dans des boîtes quantiques, duraient 10 nanosecondes. Dix ans plus tard, une microseconde, soit cent fois mieux. Maintenant, ils durent 100 microsecondes », se félicite Lieven Vandersypen. D'autres systèmes, comme des atomes piégés dans des lasers, peuvent même durer plus longtemps, mais cela reste malgré tout trop faible. Car c'est durant ce temps court qu'il faut effectuer les milliers d'opérations (quelques dizaines de nanosecondes chacune) nécessaires pour réaliser un calcul.

La correction d'erreurs, le Saint-Graal

Autre problème, toutes ces opérations peuvent entraîner des erreurs, comme dans le monde classique, qu'il convient de corriger. Dans un ordinateur, une méthode simple est la redondance. Au lieu de prendre un bit, on travaille avec trois, ce qui diminue la chance que tous les membres du trio soient affectés ensemble par une erreur… En mécanique quantique, la même chose est possible, sauf que cela augmente le nombre de qubits, et donc la difficulté. Autre problème, il faut délicatement interagir avec ces qubits correcteurs, car, on l'a vu, si on mesure leur valeur, ils perdent tout intérêt, redevenant simples bits d'information classiques. «La correction d'erreurs est le Saint-Graal du domaine », rappelle Hartmut Neven, directeur de l'ingénierie chargé de la recherche sur l'intelligence artificielle et l'informatique quantique chez Google. Des progrès ont été réalisés depuis un an. A Delft,

par exemple, en 2016, des erreurs ont été corrigées sur 3 qubits. Dans le même laboratoire, un autre groupe, en collaboration avec Microsoft, travaille, lui, sur la conception d'un qubit d'une autre nature, plus résistant aux perturbations extérieures.

Mais le salut pourrait venir d'une technique différente développée à l'université Yale, en collaboration avec l'Institut national de recherche en informatique et en automatique (Inria) en France, où les chercheurs ont réussi, en 2016, à augmenter la durée de vie de leur qubit de 10%. « Aucun code correcteur d'erreur n'a fait mieux que notre système », estime Mazyar Mirrahimi de l'Inria. «C'est impossible de contrôler des milliers de qubits », tacle Michel Dyakonov, professeur émérite à l'université de Montpellier et l'un des rares physiciens très sceptiques sur cet « engouement, aux perspectives très exagérées ». « Les spécialistes réalisent que la correction d'erreur ne sera pas aussi simple qu'on le dit», préfère déclarer Mazyar Mirrahimi.

La messe est dite ? Non, car les ingénieurs quantiques, comme leurs qubits, savent prendre plusieurs formes. Si le nombre magique de 49 qubits est un objectif consensuel chez les Google, IBM et consorts, pour démontrer la suprématie quantique, on sait que ça n'en fera pas un ordinateur universel, car ne résistant pas aux erreurs. « Cette machine fera de petites fautes, mais on la fera tourner plusieurs fois et, statistiquement, nous pourrons en

extraire des résultats », estime Hartmut Neven. D'autres plaident non pas pour ces « accélérateurs quantiques », mais pour des « simulateurs » – renouant avec les premiers concepts nés dans les années 1980. C'est-à-dire des machines qui n'utilisent pas les propriétés quantiques pour faire des calculs, mais pour reproduire des effets naturels dans la matière, qui après tout est régie par les lois de la mécanique quantique. Au Collège de France par exemple, une mélasse d'atomes froids en interaction peut simuler la surface d'une étoile à neutrons. D'autres évoquent l'étude des propriétés des matériaux pour l'énergie, les interactions moléculaires pour la biologie et la pharmacie, la physique des particules…

Autre avatar, la machine de D-Wave. Cette entreprise canadienne, née en 1999, a vendu depuis 2011 quatre calculateurs, pour une dizaine de millions de dollars (8,8 millions d'euros), à Lockheed Martin, à Google (associé à la NASA), au Laboratoire Los Alamos et à l'entreprise de cybersécurité Temporal Defense Systems. Une version en ligne est même accessible. Son dernier modèle possède plus de 2000 qubits, mais qui ne sont pas tous connectables entre eux. Le fonctionnement est intermédiaire entre l'ordinateur universel programmable et les simulateurs. Il permet d'explorer un ensemble de solutions et de trouver la meilleure. Sauf que pour l'instant, sur les problèmes résolus, on ignore s'il n'existe pas une solution plus rapide avec une méthode classique.

Une autre voie est explorée à Delft ou chez son concurrent académique d'Oxford, NQIT: relier entre eux par des fibres optiques des «petits» ordinateurs quantiques. Ces noeuds « travailleraient ensemble» en échangeant de l'information avec leurs voisins, grâce aux photons, les seuls messagers à pouvoir voyager et transférer des propriétés quantiques à la matière. Ian Walmsley, directeur du NQIT, envisage ainsi d'avoir dans les cinq à dix ans 5 noeuds de 50 qubits, contre 2 de 2 qubits aujourd'hui.

Et si ça n'est pas pour le calcul, cela servira au moins de réseaux Internet sécurisés, comme veut le démontrer QuTech en reliant, d'ici à 2020, quatre villes aux Pays-Bas. «Les protocoles de communication quantique arriveront probablement avant les gros ordinateurs », estime Iordanis Kerenidis, directeur du Paris Centre for Quantum Computing, partenaire de QuTech dans ce projet de réseau

quantique, et qui fédère les principaux spécialistes parisiens de ce nouveau domaine. «Sur ces chemins, il y aura toujours de la belle

science », rassure Julia Cramer, chargée du rayonnement du laboratoire QuTech. Si la perspective de surpasser les super-ordinateurs actuels pour des calculs complexes semble encore lointaine, l'implication des géants de l'informatique promet déjà une «victoire» prochaine sur des problèmes d'optimisation simples. L'avenir reste flou comme un qubit.

« NOUS AVONS PROGRESSÉ ET AVONS CONFIANCE : DANS LA PROCHAINE DÉCENNIE, UN ORDINATEUR QUANTIQUE UNIVERSEL SERA DÉVELOPPÉ » XAVIER VASQUES DIRECTEUR TECHNIQUE, IBM FRANCE