Le Monde science&techno

N° et date de parution : 20870 - 25/02/2012
Diffusion : 300000
Périodicité : Bi-hebdomadaire
MondeSci_20870_4_6.pdf
Site Web : http://www.lemonde.fr
Page : 4
Taille : 65 %
3764 cm2

Ordinateur quantique

Un calculateur pas encore prodige

PHYSIQUE

Le Nobel Richard Feynman a imaginé, il y a trente ans, tirer profit des étranges propriétés de la mécanique quantique pour créer une nouvelle classe d'ordinateurs. Le premier a été livré il y a quelques mois, mais son statut fait débat. Le point sur une technologie émergente, aux performances potentiellement vertigineuses

Le Monde science&techno


Ordinateur quantique
Un calculateur pas encore prodige

N° et date de parution : 20870 - 25/02/2012
Diffusion : 300000 Page : 4
Périodicité : Bi-hebdomadaire Taille : 65 %
MondeSci_20870_4_6.pdf 3764 cm2
Site Web : http://www.lemonde.fr

DENIS DELBECQ

Dates

1973 Chez IBM, Charles Bennett pose les bases d'un ordinateur réversible, capable en théorie de fonctionner sans énergie. Cela oblige à repenser les opérations logiques de base pour ne pas détruire d'informations.

1981 Le Prix Nobel de physique Richard Feynman propose d'utiliser un ordinateur quantique pour étudier le fonctionnement de systèmes quantiques.

1994 Le mathématicien Peter Shor décrit une méthode pour factoriser un nombre à l'aide d'un ordinateur quantique. Deux ans plus tard, Lov Grover montre comment trouver une information dans une base de données de manière plus efficace qu'avec un ordinateur classique.

2001 Des chercheurs d'IBM apportent la première démonstration de l'algorithme de factorisation de Shor, en calculant que le nombre 15 est le produit de 3 par 5.

2011 Le premier processeur quantique, doté d'une double unité de calcul, de mémoire et de circuits d'effacement, est présenté par l'équipe de John Martinis à l'université de Californie à Santa Barbara.

« J'offre cent mille dollars à qui me fera une démonstration convaincante qu'il est impossible de construire un ordinateur quantique dont la puissance est évolutive. » Le défi a été lancé, début février, par Scott Aaronson sur son blog. Ce spécialiste de la complexité des calculs au Massachusetts Institute of Technology (MIT) est agacé par les détracteurs de l'informatique quantique, une discipline qui espère détourner à son avantage les propriétés de la matière à l'échelle la plus intime, où règnent les ondes, atomes et particules élémentaires, pour créer des machines dont la puissance dépasse l'entendement. Alors il a jeté un pavé dans la mare. *« Qu'on ne compte pas sur moi pour lancer le défi inverse »*, écrit-il. En janvier, une firme canadienne, D-Wave, a annoncé avoir réussi un calcul sophistiqué sur son prototype d'ordinateur quantique. Mais son résultat a été fraîchement accueilli par la communauté scientifique.

L'idée d'utiliser les propriétés de la physique quantique pour faire du calcul a été exprimée pour la première fois en 1981, lors d'un congrès scientifique au MIT. Le Prix Nobel de physique Richard Feynman avait pris la parole devant une cinquantaine de chercheurs : *« Quelle sorte d'ordinateur allons-nous utiliser pour faire des simulations de physique ? »*, s'interrogeait le physicien, tout en proposant une piste de réflexion : pour étudier la physique quantique et ses lois si étranges pour le commun des mortels, il faudra mettre au point un ordinateur quantique qui obéisse aux règles qu'il entend simuler…

Trente ans plus tard, des processeurs rudimentaires sont capables de réaliser des opérations très simples, comme rechercher un numéro de téléphone dans une liste de quelques abonnés, à l'instar du système développé au sein du groupe Quantronique – pour électronique quantique – de Daniel Estève, au centre CEA de Saclay (Essonne) : *« Nous avons réalisé un processeur à deux qubits capable de retrouver, en un pas d'algorithme, une information dans un groupe de quatre, avec une probabilité de 60 %. Même s'il est possible de progresser jusqu'à 100 %, c'est déjà supérieur à un algorithme classique »*, résume le chercheur. Qubits, probabilité… inutile de le nier, l'univers de l'information quantique oblige à revoir ses concepts et son vocabulaire.

Dans un processeur classique, l'information est faite de paquets d'électrons qui voyagent dans les circuits électroniques, comme de l'eau le ferait dans un réseau de réservoirs, d'écluses et de canaux. Le réservoir est une cellule de mémoire qui stocke l'information sous forme de nombre binaire, en anglais *binary digit* ou bit : quand il est plein, il représente le 1. Vide, c'est un 0. L'écluse ? C'est un transistor, une sorte d'interrupteur télécommandé qui peut laisser passer ou bloquer le courant. Et les canaux sont les infimes fils électriques qui relient tous ces microcomposants.

Les transistors sont organisés en circuits élémentaires – on les appelle des portes – capables de réaliser des opérations logiques sur les bits : comparaison, inversion, etc. Ces portes sont à leur tour organisées de manière à produire des calculs plus complexes, comme l'addition ou la multiplication. Et ainsi de suite, jusqu'à doter les puces des fonctions sophisti-

Le Monde science&techno

N° et date de parution : 20870 - 25/02/2012
Diffusion : 300000
Périodicité : Bi-hebdomadaire
MondeSci_20870_4_6.pdf
Site Web : http://www.lemonde.fr
Page : 4
Taille : 65 %
3764 cm2

Cette discipline espère détourner à son avantage les propriétés de la matière à l'échelle la plus intime, pour créer des machines dont la puissance dépasse l'entendement

quées qui font la souplesse des ordinateurs d'aujourd'hui.

Le premier microprocesseur commercial de l'histoire, l'Intel 4004, a été lancé, en 1971, avec 2300 transistors. Certaines puces dépassent aujourd'hui le milliard de transistors. Mais personne n'a réussi à surmonter leur principal défaut : un microprocesseur ne fait qu'une ou quelques opérations à la fois, ce qui l'empêche de résoudre certains énoncés mathématiques pourtant simples.

Un exemple : imaginez un voyageur de commerce qui cherche le trajet le plus court pour visiter tous ses clients et revenir chez lui sans repasser deux fois au même endroit. Facile, se dit le VRP : il n'y a qu'à comparer toutes les possibilités. Tant qu'il n'a qu'une poignée de villes à voir, il s'en sortira avec une calculette ou avec son ordinateur. Mais, très vite, le compteur s'affole : pour vingt étapes, il y a déjà quelque dix milliards de milliards de possibles.

Notre VRP s'en tirera encore en mobilisant des dizaines de milliers d'ordinateurs reliés par Internet. Mais s'il doit visiter les 69 villes les plus importantes de France, le nombre de combinaisons comporte cent chiffres, vingt de plus que le nombre d'atomes de l'Univers... A supposer qu'un petit génie ait trouvé le moyen de transformer chacun de ces atomes en un « classique » PC de bureau et de les connecter, il faudrait trente ans de calculs avant que notre VRP puisse prendre la route.

D'où l'idée de mettre au point des machines capables d'effectuer des milliards de milliards d'opérations simultanément, pour faire progresser des domaines aussi variés que la météorologie, la physique du solide ou l'étude de la forme des protéines. C'est là que la physique quantique entre en scène. Alors qu'un bit classique peut prendre la valeur 0 ou la valeur 1, une information quantique – portée par un qubit, pour bit quantique – pourra valoir à la fois 0 et 1. Cette « superposition d'états » permise par les lois de la physique quantique se traduit par la possibilité de faire d'innombrables calculs en parallèle avec un nombre relativement restreint de qubits. Selon Franck Wilhelm-Mauch, de l'université de la Sarre (Allemagne), *« cent qubits représentent l'équivalent de 2^{100} transistors classiques »*. Un nombre de 31 chiffres qui donne un aperçu de ce que pourrait être la puissance d'un vrai ordinateur quantique, même si une grande partie des qubits servirait à corriger les erreurs et transformer les probabilités, chères à la physique quantique, en certitudes.

Aujourd'hui, il existe de nombreuses manières d'obtenir des qubits, explique Daniel Estève : ce peut être par exemple des atomes ou des ions (atomes débarrassés d'un ou de plusieurs électrons) piégés dans une cavité, des particules de lumière – les photons –, des molécules, des circuits supraconducteurs quantiques ou des électrons piégés dans des circuits semiconducteurs. Le dispositif le plus complexe a été mis au point, en 2011, par le groupe de Reiner Blatt à l'université d'Innsbruck : il comporte 14 qubits, 14 ions de calcium piégés dans une trappe, dont les propriétés sont couplées grâce à un mécanisme appelé intrication quantique : la possibilité de lier les états de plusieurs systèmes – des atomes, des ions ou des photons, par exemple – pour qu'ils forment un tout indissociable, quelle que soit la distance qui les sépare.

C'est cette intrication, ce couplage entre les qubits, qui va permettre d'effectuer de grandes quantités de calculs en parallèle. Mais elle n'est pas facile à mettre en œuvre et surtout à conserver dans le temps : chaque qubit doit être totalement isolé du reste du monde sous peine de perdre ses propriétés quantiques. *« On fait face à un phénomène baptisé "décohérence"*, explique Daniel Estève. *Aujourd'hui, elle apparaît toujours trop tôt pour avoir un processeur quantique vraiment fonctionnel. Dans le cas des circuits supraconducteurs, la décohérence apparaît au mieux après quelques dizaines de microsecondes, un temps qui semble court, mais*

Le Monde science&techno

N° et date de parution : 20870 - 25/02/2012
Diffusion : 300000 Page : 4
Périodicité : Bi-hebdomadaire Taille : 65 %
MondeSci_20870_4_6.pdf 3764 cm2
Site Web : http://www.lemonde.fr

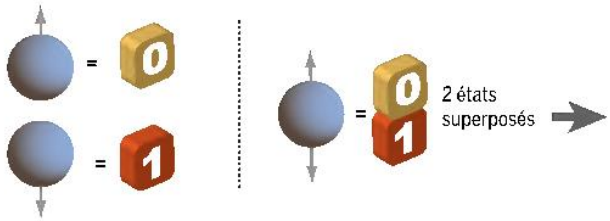
Press Index

Des qubits pour faire plus avec moins

Le qubit ou bit quantique

La mémoire d'un ordinateur quantique travaille avec des particules appelées **qubits,** cases mémoire où l'information est stockée sous forme de 0, de 1, ou **les deux à la fois.**

Particule Information **Superposition quantique**



A l'échelle moléculaire, la mécanique quantique autorise l'ubicuité des objets. Une particule peut avoir **deux états** à la fois.

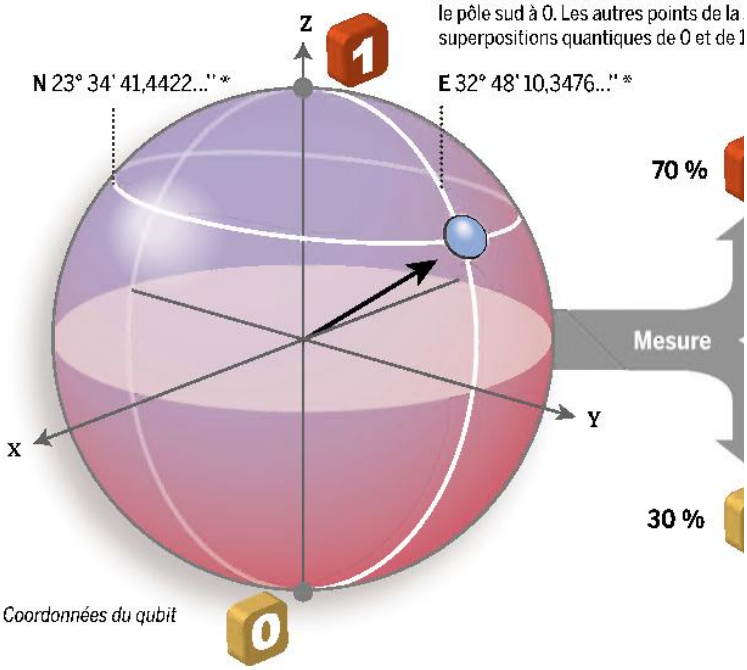
Le bit

La mémoire d'un ordinateur classique est composée de bits. C'est la plus petite unité d'information manipulable par une machine numérique de type ordinateur individuel.

Un bit peut stocker **une seule** information à la fois : 0 ou 1.

Sphère de Riemann

Les états d'un qubit peuvent être repr
pointant un lieu sur une sphère. Le pôl
le pôle sud à 0. Les autres points de la
superpositions quantiques de 0 et de 1



sentés par une flèche
nord équivaut à 1.
sphère sont des

Un qubit peut sembler contenir une infinité d'informations, parce que les coordonnées qu'il présente peuvent encoder une séquence infinie de chiffres.

Mais cette information doit être extraite lors d'une mesure. Et lorsque cette mesure est effectuée, la mécanique quantique requiert que le résultat soit toujours un bit ordinaire (un 0 ou un 1).
La probabilité de ces deux résultats dépend de la « latitude » du qubit.

Une puissance de calcul exponentielle

Nombre de qubits
1
2
3
4
5
...

Nombre de bits ⇒	Nombre d'états possibles
2 (00/01/10/11)	4
4	16
8	64
16	256
32	1024
...	...

n qubits <=> 2^n bits
⇒ 2^{2n} combinaisons

La machine D-Wave

Conçu par une société canadienne, ce calculateur spécialisé fonctionnerait avec un processeur quantique comprenant 128 qubits. Un exemplaire a été livré à l'automne 2011 à l'université de Californie du Sud.

Le Monde science&techno


Ordinateur quantique
Un calculateur pas encore prodige

N° et date de parution : 20870 - 25/02/2012
Diffusion : 300000
Périodicité : Bi-hebdomadaire
MondeSci_20870_4_6.pdf
Site Web : http://www.lemonde.fr
Page : 4
Taille : 65 %
3764 cm2

tout de même bien plus long que celui d'une opération logique entre qubits.»

Sur le papier, l'ordinateur quantique pourrait être polyvalent. L'Américain Peter Shor a ainsi montré, en 1994, qu'il pourrait factoriser des grands nombres – découvrir les nombres, qui, multipliés entre eux, donnent le nombre de départ. Un calcul si gourmand en puissance que c'est sur lui que reposent les systèmes de cryptographie classiques pour sécuriser les transactions bancaires sur Internet et déjouer les espions. Mais l'ordinateur quantique n'en est pas encore là : en 2001, une équipe d'IBM a déterminé que 15 est le produit de 3 par 5. C'est certes à la portée d'un enfant de primaire, mais c'est la première application concrète de la méthode de Peter Shor. Une équipe chinoise aurait décomposé 143 en 11 fois 13, mais en utilisant une astuce propre à ce nombre.

En septembre 2011, le groupe de John Martinis, à l'université de Californie à Santa Barbara, a réalisé un coup d'éclat en annonçant dans *Science* ce qui semble bien être le premier processeur quantique imitant les puces classiques : deux qubits capables de communiquer, deux cellules de mémoire quantique et deux circuits capables d'effacer ces mémoires. Trois types de circuits qui, ensemble, répondent à la définition de ce qu'est un microprocesseur. Ils logent dans un carré de six centimètres de côté. La puce a permis de faire plusieurs calculs mathématiques, dont la célèbre transformée de Fourier, très utilisée en traitement de signal (image, son, télécommunications, etc.).

Un résultat honoré par la revue spécialisée *Physics World*, qui l'a placé dans son top 10 des découvertes de l'année 2011. Tout comme le groupe de Daniel Estève au CEA, l'équipe californienne fabrique ses qubits à l'aide d'une jonction Josephson. Il s'agit d'un petit composant formé de deux éléments supraconducteurs séparés par un mince isolant, le tout étant refroidi à – 273,13 °C, vingt millièmes de degré au-dessus du zéro absolu ! *« L'avantage de ces dispositifs microfabriqués, c'est que, si on sait en produire un, on peut en faire beaucoup et les intégrer »*, se réjouit Daniel Estève. Ces circuits « quantroniques » laissent envisager une montée en puissance rapide. *« On devrait atteindre dix qubits dans un avenir très proche »*, prédit le physicien, tandis que son collègue John Martinis pronostique qu'*« avec cent à mille qubits il sera possible de faire des expériences vraiment intéressantes. Nous testons une nouvelle puce avec trois qubits dont le temps de cohérence est nettement meilleur qu'aujourd'hui ».*

« Il ne faut pas se leurrer, ce sont de belles expériences, mais il s'agit encore de recherches très fondamentales », prévient Serge Haroche, professeur au Collège de France, dont le groupe à l'Ecole normale supérieure de Paris travaille dans une direction différente. Quelques photons sont piégés entre des miroirs dans une cavité et interagissent avec des atomes qui sont introduits un par un pour contrôler le nombre de photons et éventuellement le corriger. Une manière d'éviter la décohérence qui détruit l'information quantique. *« Cela nous permet d'avoir une très grande stabilité dans le temps. Dès qu'un photon disparaît parce qu'il est absorbé, les atomes "contrôleurs" introduisent un photon remplaçant, créant ainsi un système robuste qui devrait permettre de réaliser des opérations quantiques complexes. »*

Mais, pour le physicien, il s'agit d'expériences qui permettent de mieux comprendre les phénomènes, plus que de concevoir les briques d'un futur supercalculateur quantique. *« On joue avec quelques qubits ; peut-être arrivera-t-on à quelques dizaines. Mais j'ai du mal à imaginer qu'on puisse aller bien au-delà, à cause de la décohérence. Le rêve du théoricien peut vite tourner au cauchemar pour l'expérimentateur. »* En revanche, Serge Haroche est persuadé que l'objectif de Richard Feynman est atteignable : *« On sait par exemple disposer quelques centaines d'atomes dans un réseau formé par l'intersection de faisceaux lasers, ce qui revient à réaliser un simulateur quantique bien plus efficace qu'un ordinateur pour étudier les interactions entre ces atomes. »* Franck Wilhelm-Mauch est plus optimiste. *« Il y a dix ans, on entendait dire qu'il faudrait une vie avant de voir un premier processeur quantique supraconducteur, et aujourd'hui il existe. Dans deux ans, on devrait avoir des systèmes à cinq ou sept qubits. On verra bien dans quelle proportion les problèmes de décohérence sont amplifiés. »*

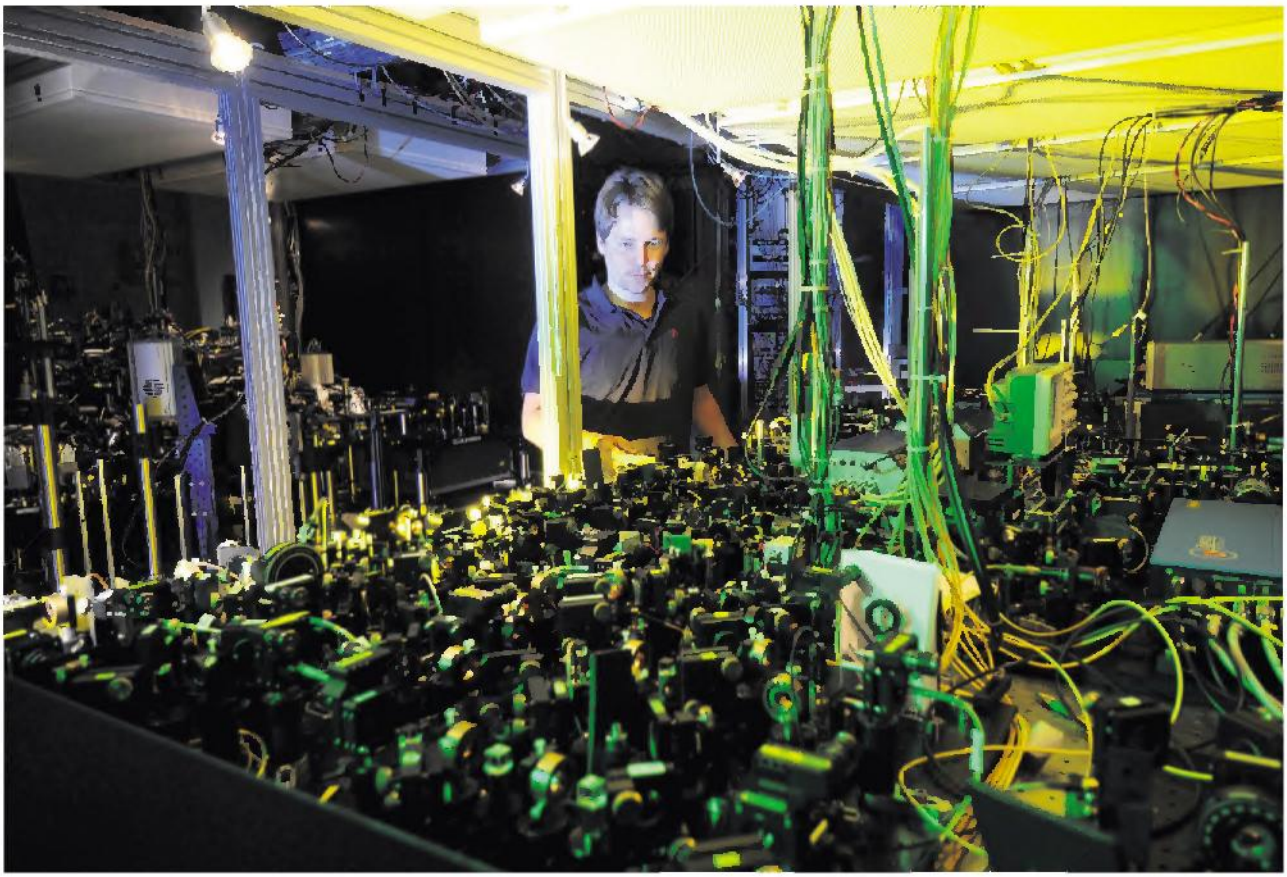
Alors qu'un bit classique peut prendre la valeur 0 ou la valeur 1, une information quantique pourra valoir à la fois 0 et 1

Sans attendre de savoir, l'équipe d'Anton Zeilinger à l'université de Vienne (Autriche) vient de réussir un calcul quantique sans que le propriétaire du processeur puisse savoir quelles opérations se déroulent. Un savant mélange de calcul et de cryptographie quantiques qui pourrait avoir son utilité, confirme Serge Haroche : *« Le calcul "aveugle" de l'équipe de Zeilinger trouve sa justification pratique dans la difficulté même du calcul quantique. Si des ordinateurs quantiques existent un jour, ils seront si difficiles à construire qu'il y en aura probablement peu, installés dans des centres de calcul. Les utilisateurs devront y envoyer leurs qubits et recevoir les résultats des calculs, tout en étant assurés que les opérateurs de la machine seront incapables d'en extraire de l'information… »* On l'aura compris : ceux qui espèrent disposer un jour de puissance quantique dans leur cartable feraient mieux de partir à la chasse au yéti. ■

Le Monde science&techno


Ordinateur quantique
Un calculateur pas encore prodige

N° et date de parution : 20870 - 25/02/2012
Diffusion : 300000
Périodicité : Bi-hebdomadaire
MondeSci_20870_4_6.pdf
Site Web : http://www.lemonde.fr
Page : 4
Taille : 65 %
3764 cm2



Montage expérimental pour construire un ordinateur quantique, à l'Institut Max-Planck d'optique quantique, à Garching (Allemagne).

THORSTEN NAESER/MPQ