cnrs le journal

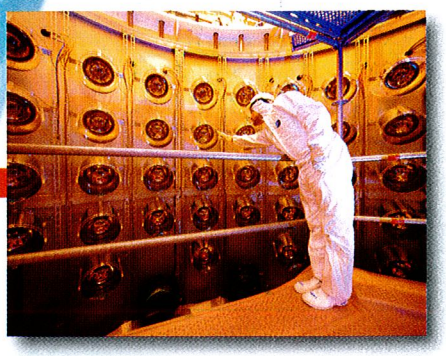
n° 250
novembre 2010

JUSQU'OÙ IRA l'informatique ?

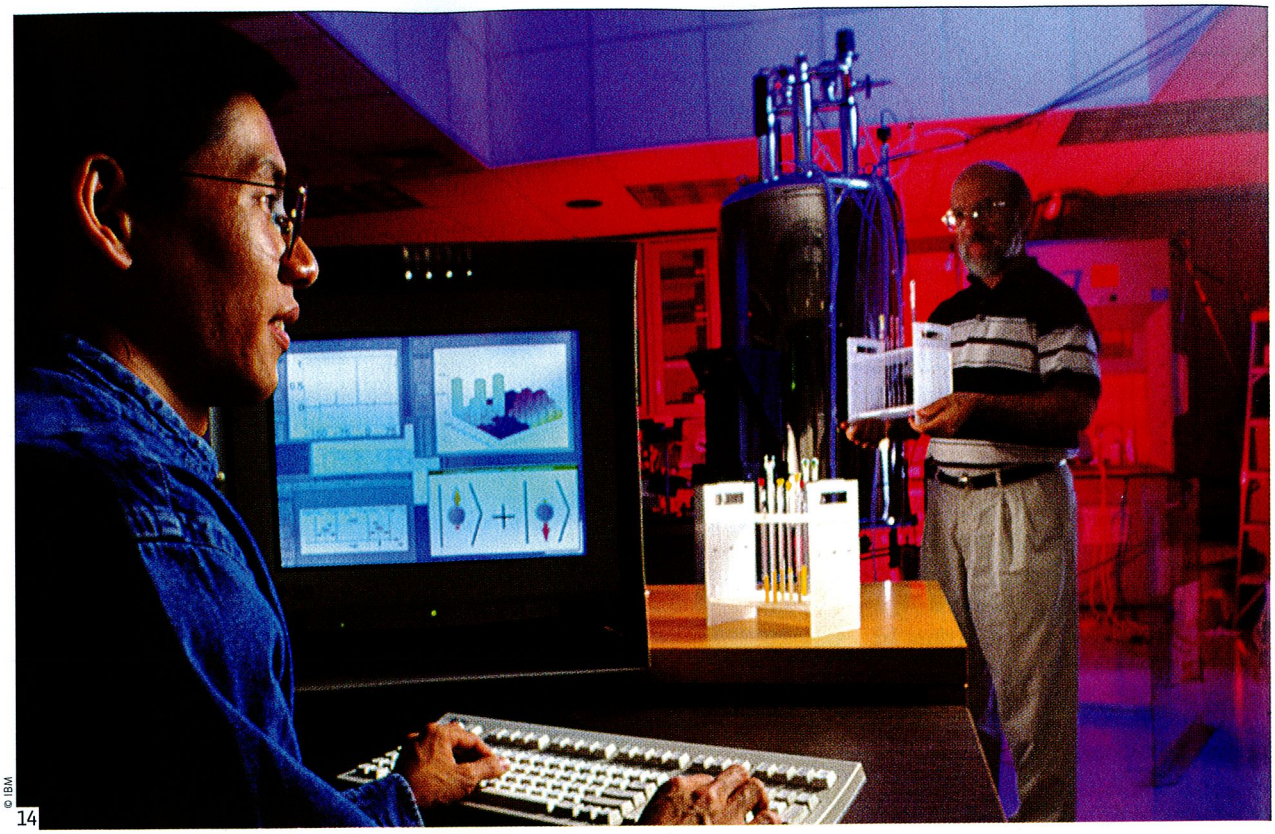
D'INTERNET À L'ORDINATEUR QUANTIQUE

L'événement

Double Chooz : la traque des neutrinos est lancée



cnrs
dépasser les frontières



© IBM

14

Ordinateur quantique : l'ultime défi

C'est un rêve d'informaticien... Un ordinateur si rapide que casser un code, prévoir la météo à long terme ou battre à plate couture n'importe quel grand maître des échecs ne lui prendrait pas plus d'une seconde. Disons le tout net, ce fantasme est loin d'être une réalité. Ce qui n'empêche pas mathématiciens et physiciens de commencer à esquisser les contours de ce que sera peut-être un jour cette extraordinaire machine. Son nom ? L'ordinateur quantique. Son concept ? Tirer partie des étonnantes lois quantiques qui autorisent une particule, un atome ou une molécule, à occuper deux états en même temps. À la manière du chat imaginé en 1935 par Erwin Schrödinger, l'un des pères de la mécanique quantique, à la fois mort et vivant. Ainsi, alors que, dans un ordinateur ordinaire, les informations sont stockées sous la forme de bits prenant les valeurs 0 ou 1, des bits quantiques (ou qubits) pourraient simultanément prendre les valeurs 0 et 1. L'intérêt : la possibilité de stocker, en principe, sur la même mémoire des informations représentant un grand nombre de solutions potentielles d'un problème. Et, en appliquant des algorithmes adaptés, traiter toutes ces solutions de concert. De quoi renvoyer les plus puissants calculateurs d'aujourd'hui à la préhistoire de l'informatique.

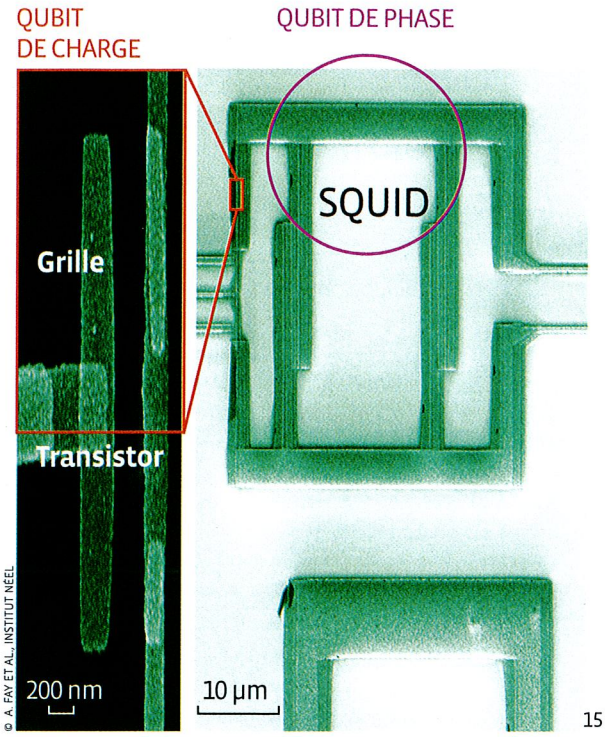
FACTORISATION Décomposition en facteurs premiers des grands nombres.

QUBIT Bit quantique qui a la particularité d'avoir un état dit de superposition où les valeurs 0 et 1 sont prises en même temps, en plus des valeurs standard 0 et 1 du bit classique.

UNE IDÉE QUI A FAIT SON CHEMIN

Pour autant, un tel ordinateur sortira-t-il jamais des laboratoires ? Et si c'était un jour le cas, serait-il vraiment capable de tous les prodiges ? Rien n'est moins sûr. Après tout, au début des années 1980, l'ordinateur quantique n'était qu'une idée lancée en l'air par le prix Nobel de physique Richard Feynman. Comme le raconte Julia Kempe, du Laboratoire de recherche en informatique (LRI), à Orsay, élue Femme en or de la recherche 2010, « *Feynman a fait remarquer qu'avec un ordinateur quantique on pourrait calculer bien plus rapidement les propriétés d'une assemblée de particules quantiques, des électrons par exemple, qu'avec un ordinateur classique. On pourrait en effet encoder chaque électron sur un qubit, alors qu'il faut une grande quantité de bits classiques pour encoder les nombreux états dans lesquels il peut se trouver en même temps. Mais ce n'était qu'une idée.* » À dire vrai, une très bonne idée. Car, en 1994, Peter Shor, alors aux Laboratoires AT & T, aux États-Unis, montre formellement qu'un ordinateur quantique pourrait factoriser un nombre, c'est-à-dire le décomposer en un produit de nombres premiers en un temps record. De quoi faire de l'ordinateur quantique la bête noire de tous les cryptographes, puisque, du fait de sa gourmandise en temps de calcul, la factorisation est actuellement la clé de tous les codes secrets, de celui de nos cartes bleues à ceux permettant d'échanger des secrets d'État. De même, en 1997, Lov Grover, des laboratoires Bell, démontre qu'un ordinateur utilisant des qubits pourrait considérablement augmenter l'efficacité des algorithmes utilisés pour la recherche d'informations dans une base de données.

Sauf que si, dans les années 1990, mathématiciens et physiciens commencent à démontrer l'intérêt de disposer d'un ordinateur quantique, la "bête" elle-même n'est encore qu'une chimère. De fait, aujourd'hui comme hier, personne ne sait concrètement de quoi seront composés les fameux qubits : des atomes ou des ions, des molécules, des électrons, des



14 L'ordinateur quantique, comme celui des chercheurs du Massachusetts Institute of Technology, à base de molécules organiques, reste pour le moment très expérimental.
15 Certains circuits supraconducteurs permettent d'analyser et de tester les nouvelles propriétés de la nanoélectronique quantique.

circuits supraconducteurs ? Sur un support solide, liquide ou gazeux ? Mystère. De nombreuses équipes à travers le monde expérimentent actuellement toutes sortes de supports matériels susceptibles d'être utilisés comme composants de base d'un futur processeur quantique. Par exemple, explique Bernard Barbara, de l'Institut Néel, à Grenoble, « *nous étudions actuellement des qubits dont les deux états 0 et 1 correspondent aux états de spin* [sorte de rotation de la particule sur elle-même] *de molécules ou d'ions de certains métaux dans des matrices solides* ».

PRINCIPAL OBSTACLE : LA DÉCOHÉRENCE

Mais, loin d'être en mesure de proposer un ordinateur clé en main, les physiciens tentent pour le moment de comprendre et, dans la mesure du possible, de contrôler l'écueil principal sur le chemin du calculateur quantique : la décohérence. Comme le détaille le spécialiste, « *tout système dans une superposition quantique de différents états est extrêmement fragile. Ainsi, sous l'effet de ses interactions avec l'environnement, il peut perdre en une fraction de seconde les propriétés nécessaires à tout calcul quantique. Et cela est d'autant plus vrai que ce système contient plus de qubits* ».

DÉCOHÉRENCE Temps pendant lequel les propriétés d'un système quantique ne sont pas corrompues par l'environnement extérieur.

À ce jour, la plus belle prouesse calculatoire réalisée avec des qubits est l'œuvre d'Isaac Chuang, de l'Institut de technologie du Massachusetts. En 2001, en utilisant le spin du noyau de sept atomes d'une molécule, ce chercheur est parvenu à factoriser 15, soit à montrer que ce nombre se décompose en 3 fois 5. « *Or, pour être performant,* indique Bernard Barbara, *un ordinateur quantique devra comporter quelques milliers de qubits. Et offrir la possibilité de les coupler afin de réaliser des calculs logiques.* »

De l'avis général, deux systèmes offrent aujourd'hui les perspectives les plus intéressantes. D'une part, les qubits supraconducteurs, soit de microscopiques circuits électroniques dans lesquels un courant électrique peut en même temps circuler dans un sens ou dans l'autre : « *Ils offrent l'avantage d'une grande facilité de fabrication. Il est donc aisé de les dupliquer et de disposer de puces comprenant de nombreux qubits supraconducteurs* », explique le physicien. Mais surtout, d'autre part, « *les ions gazeux piégés par de puissants faisceaux lasers, avec lesquels on obtient des temps de cohérence de plusieurs minutes malgré des systèmes encore relativement restreints* ». « *L'ordinateur quantique n'est pas pour demain,* confie Bernard Barbara. *Mais je pense que d'ici à quelques dizaines d'années il pourrait devenir une réalité.* » Miklos Santha, lui aussi du LRI, est plus nuancé : « *Qui sait si nous ne finirons pas par découvrir que la nature interdit la possibilité même d'un ordinateur quantique…* »

LES RECHERCHES CONTINUENT

Et, quand bien même, celui-ci ne serait pas exactement l'ordinateur ultime. Car seules certaines catégories de problèmes pourraient voir leur résolution accélérée par un ordinateur quantique. « *Certes, le gain est considérable dans le cas de la factorisation. Mais il l'est déjà moins dans le cas de la recherche de données non triées,* reconnaît Miklos Santha, *de même que pour déterminer l'itinéraire le plus court sur une carte, ou bien pour le jeu d'échec ou le Go. Et quasi nul pour d'autres types de données. Il y a quelques grands miracles, mais ils sont rares.* » De quoi rendre vaine toute recherche sur l'ordinateur quantique ? Loin de là. En effet, comme le précise Bernard Barbara, « *que nous construisions ou pas un ordinateur quantique, nos recherches permettent d'apprendre à maîtriser les lois quantiques et de mieux en comprendre les fondements* ».

Quant à Julia Kempe, elle insiste sur l'intérêt de développer des algorithmes quantiques : « *Ils constituent des outils mathématiques très performants pour aborder des questions fondamentales liées à la complexité. Mais aussi pour étudier ce qu'un ordinateur classique peut faire ou ne pas faire. Enfin, les algorithmes quantiques de factorisation sont à la base du développement de la cryptographie quantique qui est déjà utilisée pour l'échange de données secrètes.* » Ainsi, personne ne sait si l'ordinateur quantique sortira un jour des laboratoires. Peu importe, même inatteignable, il demeure une source d'inspiration sans fin. Bref, un véritable rêve de scientifique.

Pour en savoir +

À LIRE |

L'Informatique en France
De la Seconde Guerre mondiale au Plan Calcul
Pierre-Éric Mounier-Kuhn, Pups, coll. « Roland Mousnier », 2010

Pourquoi et comment le monde devient numérique
Gérard Berry, Collège de France/ Fayard, 2008

À VOIR |

Jacques Stern ou la science du secret
(2006, 15 min), réalisé par François Tisseyre, produit par CNRS Images

Marc-Olivier Killijian roboticien
(2010, 5 min), réalisé par Didier Boclet, produit par CNRS Images

Émergence d'un nouveau monde
(2006, 53 min), réalisé par Jean-Pierre Mirouze, produit par Flight Movie et CNRS Images

CONTACT | Véronique Goret, CNRS Images-Vidéothèque
Tél. : 01 45 07 59 69
› videotheque.vente@cnrs-bellevue.fr
› http://videotheque.cnrs.fr

+ WEB
Des **photos** et des **films** sont à découvrir sur le journal feuilletable en ligne
› www2.cnrs.fr/journal

CONTACTS :
Bernard Barbara
› bernard.barbara@grenoble.cnrs.fr
Julia Kempe
› julia.kempe@lri.fr
Miklos Santha
› miklos.santha@lri.fr