

N° 29 - TRIMESTRIEL NOVEMBRE 2007

LES DOSSIERS DE LA RECHERCHE

LES DOSSIERS

DE La Recherche

Le monde quantique

Les nouvelles frontières
de la physique



Les constructeurs de qubits

L'ordinateur quantique n'est plus seulement théorique. Son unité de calcul, le qubit, pourrait être portée par des ions piégés et refroidis à très basse température. Cette technique permet déjà de réaliser des calculs simples.



Ferdinand Schmidt-Kaler

est professeur à l'université d'Ulm, en Allemagne.

ferdinand.schmidt-kaler@uni-ulm.de

Philippe Grangier

est directeur de recherche à l'Institut d'optique, à Palaiseau.

philippe.grangier@institutoptique.fr

Avec des dimensions de quelques dizaines de nanomètres, les transistors des ordinateurs actuels ne sont plus très éloignés de l'échelle atomique où apparaissent les propriétés quantiques des constituants élémentaires de la matière. Dans le cadre technologique actuel, ces effets quantiques sont le plus souvent considérés comme une nuisance, source d'erreurs de calcul. Le principe d'un ordinateur quantique consiste au contraire à exploiter ces propriétés : il s'agit de concevoir de nouveaux processeurs dont

la puissance de calcul pourrait être augmentée exponentiellement. Dans cette nouvelle approche, les bits, unités élémentaires de l'informatique classique, deviennent des bits « quantiques », des qubits, le plus souvent portés par des objets quantiques individuels, par exemple des atomes, des ions ou des photons. De nombreuses équipes de recherche parviennent déjà à manipuler ces qubits et à leur faire effectuer des opérations simples, premiers pas vers des calculs complexes. Dans son principe, un calcul quantique équivaut à faire



évoluer de manière contrôlée l'état initial d'un ensemble de qubits (appelé un q-registre). À la fin du calcul, on mesure l'état du q-registre, qui fournit une valeur binaire comme pour un registre classique. Bien qu'il commence et se termine tel un calcul classique, le calcul quantique est d'une extraordinaire puissance. Il possède en effet une propriété inimaginable dans le monde classique : pendant le calcul lui-même, l'ordinateur met parallèlement en jeu tous les états correspondant à tous les nombres que le registre peut contenir.

Pour contrôler cette méthode de calcul paradoxale, on doit faire évoluer le système de qubits sous l'action d'une horloge qui détermine le rythme du calcul. À première vue, une opération compliquée, notamment la factorisation de très grands nombres (lire « Comment calculer quantique », p. 50), semble être un problème inextricable. En réalité, ce calcul peut être décomposé en une succession d'opérations simples n'affectant qu'un ou deux qubits. Elles sont effectuées par des « portes logiques », dont des exemples bien connus en informatique classique sont les portes NON, ET, OU, etc. Mais, puisque les portes quantiques agissent sur des qubits, elles peuvent effectuer certaines opérations logiques inconcevables classiquement. En particulier, parce que l'information n'est pas portée par chaque qubit, mais par des corrélations quantiques entre plusieurs d'entre eux. Cette « intrication » des qubits joue un rôle fondamental dans ce type de calcul.

Ions piégés

Le passage à la réalisation d'un ordinateur quantique requiert de combiner deux exigences a priori contradictoires. D'une part, il est indispensable, afin d'effectuer le calcul désiré, de pouvoir agir sur les qubits, de les intriquer et les faire interagir. D'autre part, il faut les

isoler le mieux possible de toutes les interactions non contrôlées avec le monde extérieur. Car l'ensemble de ces interactions, que l'on appelle « décohérence », détruit le caractère quantique – et en particulier l'intrication – de l'état du registre (lire « La décohérence livrera-t-elle tous ses secrets ? », p. 22). Il induit des erreurs dont l'accumulation peut rapidement devenir inacceptable, car elle empêche le calcul d'aboutir.

Malgré la difficulté prévisible de telles opérations, le nombre de can-

vent être excités ou laissés dans leur état fondamental. Leur état d'excitation, noté « 0 » ou « 1 », devient une unité élémentaire d'information quantique, c'est-à-dire un qubit. Le calcul est effectué en utilisant des faisceaux lasers focalisés sur chacun des ions. Ceux-ci, convenablement ajustés, permettent de préparer les qubits dans l'état souhaité (« 0 » ou « 1 »), de piloter le déroulement du calcul et, finalement, de lire l'état du registre, en forçant l'ion à émettre une lumière qui va révéler son état « 0 » ou « 1 » [fig. 1].

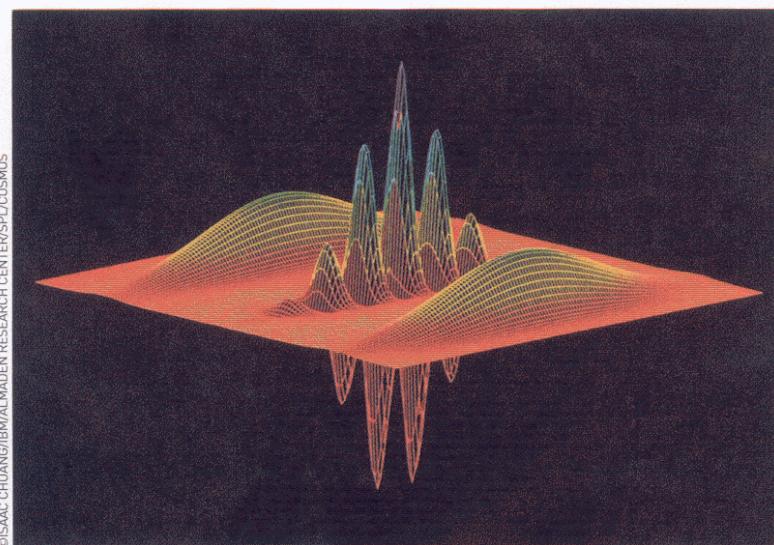
Les techniques expérimentales doivent beaucoup aux lauréats du prix Nobel de physique

didats au titre de qubit est actuellement très grand (lire « Les autres candidats qubits », p. 63). Un sondage réalisé par le site Web QubitNews [1] place les ions, s'ils sont piégés dans un petit volume par des champs électriques, en tête des candidats potentiels : il est alors effectivement possible de les contrôler, de les coupler et de les protéger des perturbations indésirables dues à leur environnement. Ces ions peu-

Ces techniques expérimentales très sophistiquées doivent beaucoup à différents lauréats du prix Nobel de physi-

que. À Theodor Hänsch et John Hall (Nobel 2005), qui ont réalisé des expériences de métrologie de grande précision, comme celles sur les horloges atomiques. À Wolfgang Paul (Nobel 1989), le père des pièges à ions, qui permettent de conserver les ions dans un volume restreint en utilisant une combinaison de champs électriques statiques et oscillants. Et également à Claude Cohen-Tannoudji, ►

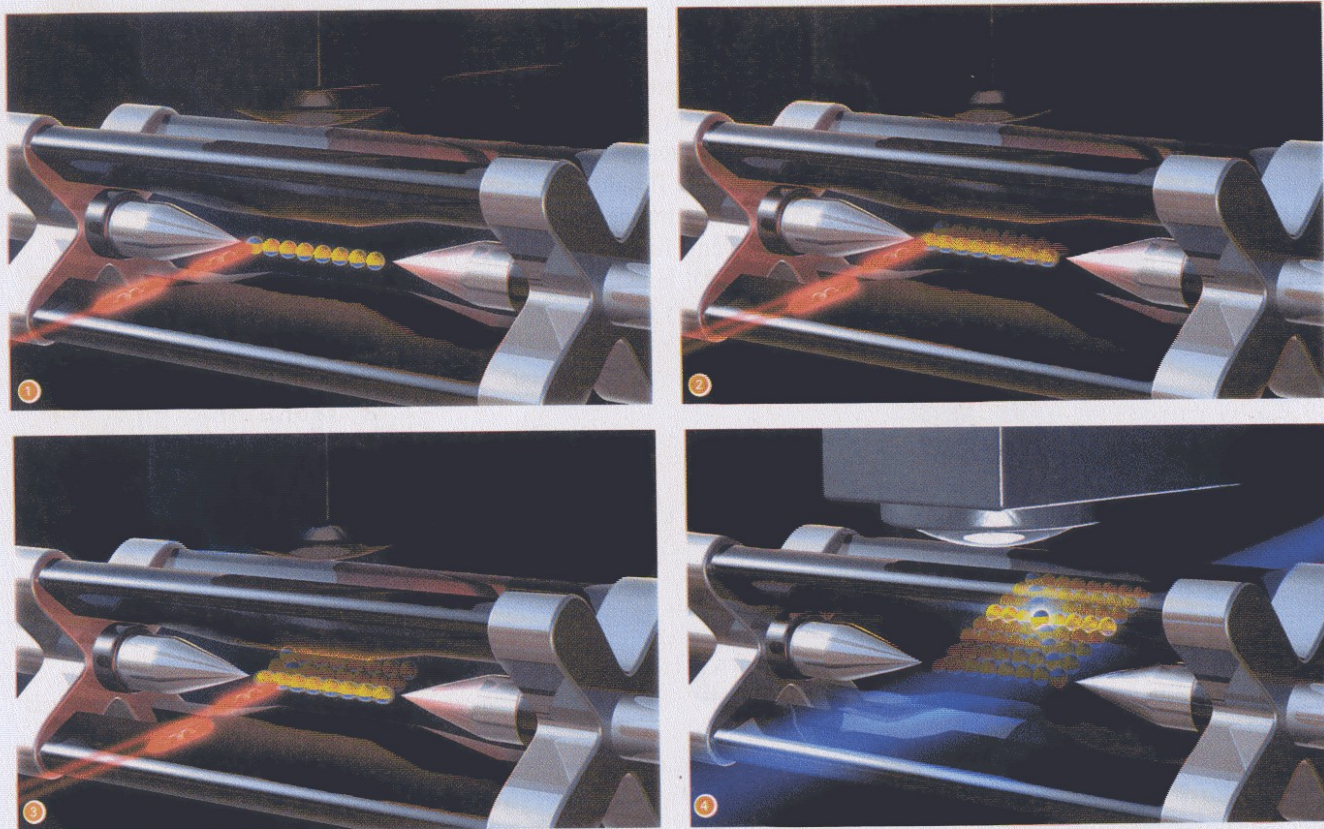
[1] <http://quantum.fis.ucm.es/pollBooth.pl?section=&qid=6&aid=-1>



LA SUPERPOSITION des états d'un bit quantique (ici, une molécule) pendant un calcul est représentée sur ce graphique. Comme le chat mort et vivant de Schrödinger, il peut être à la fois en position haute et basse.



Fig. 1 Huit ions piégés pour un calcul quantique



ILLUSTRATIONS : WWW.GREGGIRADE.COM

LA PRÉPARATION DU Q-REGISTRE, qui sert de support aux calculs, fait intervenir un faisceau laser. Au début, les huit ions sont dans le même état quantique (représenté par la couleur bleue). Une première impulsion laser fait tourner le premier ion ①. Son état quantique change. Une deuxième impulsion remet le premier ion dans son état de base et fait bouger tous les ions qui deviennent intriqués ②. Les ions sont maintenant dans deux états à la fois. Puis

une impulsion laser touche le deuxième ion qui change à son tour d'état ③. Progressivement les huit ions vont subir le même sort. L'ensemble des ions sera ainsi dans huit états quantiques simultanément. Le calcul ayant été réalisé par des manipulations de ces états, le résultat se lit par un laser d'une autre longueur d'onde, qui éclaire l'ensemble des ions et les « décohère ». Un seul ion va émettre de la lumière par fluorescence. Son état donne le résultat ④.

► Steven Chu et William Phillips (Nobel 1997), dont le travail sur le refroidissement par laser est important dans ces expériences de calcul quantique, car l'amplitude du mouvement des ions piégés – donc leur température – doit être diminuée jusqu'à ce qu'elle atteigne une dizaine de nanomètres, limite quantique imposée par le principe d'incertitude de Heisenberg (lire « Que veulent dire les inégalités de Heisenberg », p. 46 et « Le principe d'indétermination », p. 44). Et pour obtenir un q-registre, ce sont plusieurs ions qui doivent être refroidi-

dis dans le même piège. Puisqu'ils portent tous la même charge positive, ils vont alors se repousser et s'arranger régulièrement dans le piège. Si la structure de ce dernier les force aussi à s'aligner, on obtient alors un piège linéaire, dans lequel les ions individuels sont séparés de quelques micromètres.

C'est cette proximité qui va permettre la réalisation du calcul. En effet, une opération logique revient à modifier l'état d'un qubit en fonction de l'état d'un autre qubit. L'idée fondamentale rendant possible la réalisation de ces opérations a été

introduite en 1995 par Ignacio Cirac et Peter Zoller, à l'université d'Innsbruck, en Autriche [2]. De manière simplifiée, elle consiste à utiliser le fait que, si un ion est mis en mouvement par un laser, il va pousser les autres à cause de sa charge électrique. En termes plus sophistiqués, les modes d'oscillation de la chaîne d'ions servent de bus quantique, capable de véhiculer l'information quantique entre les qubits portés par les ions piégés. Les mouvements d'oscillations étant eux-mêmes quantifiés, ils s'effectuent par « sauts » soigneusement



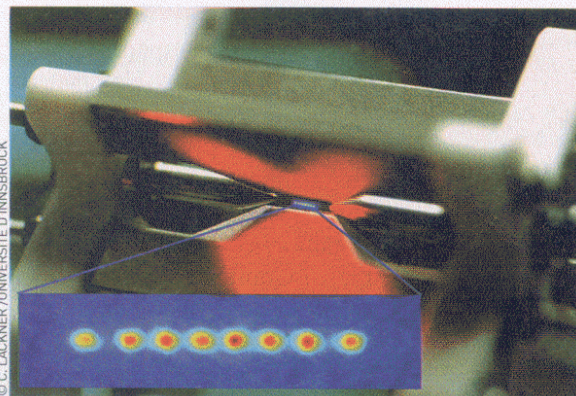
contrôlés : par exemple, si un ion est dans l'état « 0 », il en déplacera un autre, mais pas s'il est dans l'état « 1 ». Il faut bien sûr se souvenir que, puisqu'un qubit peut être à la fois dans l'état « 0 » et dans l'état « 1 », il va à la fois pousser et ne pas pousser son voisin... ce qui illustre les limites des représentations imagées du fonctionnement de ce système (voir graphique, p. 61). Néanmoins, la chaîne d'ions peut être à nouveau complètement immobilisée après chaque opération logique, ce qui assure le bon déroulement du calcul.

Les expériences réalisées par les groupes de Rainer Blatt, à l'université d'Innsbruck, et de Dave Wineland, du National Institute of Standards and Technology (NIST) de Boulder, dans le Colorado, ont ainsi permis de passer rapidement

de la réalisation de la première porte à 2 qubits en 2003 [3], à la mise en œuvre d'un petit algorithme à 3 qubits l'année suivante [4], puis à celle d'un état intriqué à 8 qubits en 2005 [5].

Corriger les erreurs

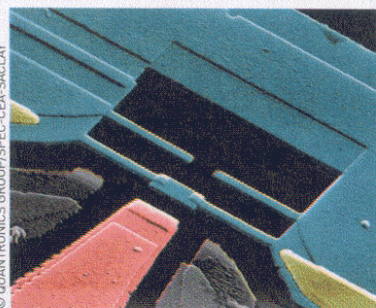
Pas encore de quoi pavoiser. Car la réalisation de calculs complexes n'est pas à la portée des expérimentateurs. Cela demande en premier lieu de maîtriser la « décohérence » : toute interaction incontrôlée du registre avec son « environnement » perturbe le fragile état intriqué et crée des erreurs dans le calcul. Il faut donc corriger ces erreurs. De nombreuses approches ont été proposées pour y parvenir. L'idée consiste à écrire un « qubit logique » non pas sur un ion unique, mais sur plusieurs



© C. LACKNER / UNIVERSITÉ D'INNSBRUCK

DANS LE LABORATOIRE DE RAINER BLATT, à Innsbruck, les ions sont piégés dans un petit volume par un champ électrique et alignés par un champ magnétique. Observés par fluorescence (en bas), ils ne sont alors écartés que de quelques micromètres, une faible distance qui leur permet de s'intriquer et d'interagir.

ions à la fois. Ce petit ensemble d'ions est effectivement plus résistant aux perturbations. Des expériences réalisées à Boulder [6] ▶



© QUANTRONICS GROUP/SPRAC-CEA-SACLAY

LE QUANTRONIUM est une puce en silicium utilisant 3 nanojonctions Josephson. Il a été mis au point en 2001 par le CEA. Deux jonctions servent de qubit, la troisième d'instrument de mesure lorsqu'un courant la traverse.

nanojonctions Josephson (des barrières à travers lesquelles un courant peut passer par effet tunnel), ou pour les qubits utilisant des états électroniques ou des états de spin dans des boîtes quantiques semi-conductrices. Ces systèmes « solides » offrent, à plus de dix ans, des perspectives intéressantes d'intégration à grande échelle.

LES AUTRES CANDIDATS QUBITS

PHOTONS POLARISÉS. Ce sont d'excellents qubits, très résistants à la décohérence, et qui peuvent se propager sur de grandes distances. Ces qualités sont à l'origine du succès de la cryptographie quantique. En revanche, il est difficile de coupler entre eux deux photons polarisés pour réaliser une porte quantique. Cela impose des contraintes fortes sur les architectures des calculateurs.

OPTIQUE QUANTIQUE. Cet ensemble de méthodes utilise les interactions entre atomes et photons. Par exemple, on peut coupler des photons entre eux en utilisant comme intermédiaires des atomes placés dans des résonateurs appropriés. C'est le domaine de l'électrodynamique quantique en cavité, qui est maintenant associée à des techniques de piégeage et de refroidissement d'atomes ou d'ions. Ces approches utilisent des objets quantiques élémentaires (atome,

ion, photon), très bien contrôlés au niveau individuel, et pour lesquels les effets de décohérence sont bien maîtrisés. Elles sont certainement très bien placées pour la réalisation d'algorithmes quantiques dans les quelques années à venir.

RÉSONANCE MAGNÉTIQUE NUCLÉAIRE (RMN). La RMN est la technique qui a permis de réaliser les premiers algorithmes quantiques et, en particulier, de « factoriser 15 » en 2001. Cependant, elle ne permet pas de réaliser un ordinateur quantique à grande échelle, en raison de difficultés pour synthétiser les molécules adéquates et pour extraire le signal utile de l'échantillon.

LES QUBITS SOLIDES. Les ordinateurs actuels étant fondés sur des puces en silicium, il est naturel d'envisager l'utilisation de techniques issues de la physique du solide. C'est le cas pour les circuits électriques supraconducteurs contenant des

[2] I. Cirac et P. Zoller, *Phys. Rev. Lett.*, 74, 4091, 1995.

[3] F. Schmidt-Kaler et al., *Nature*, 422, 408, 2003; D. Leibfried et al., *Nature*, 422, 412, 2003.

[4] M. Riebe et al., *Nature*, 429, 734, 2004; M. D. Barrett et al., *Nature*, 429, 737, 2004.

[5] H. Häffner et al., *Nature*, 438, 643, 2005.

[6] D. Kielpinski et al., *Science*, 291, 1013, 2001; J. Chiaverini et al., *Nature*, 432, 602, 2004.



[7] H. Haffner et al., *Appl. Phys. B*, 81, 151, 2005.

[8] I. Cirac et P. Zoller, *Nature*, 404, 579, 2000.

► et à Innsbruck [7] utilisent cette notion de « sous-espace préservé de la décohérence ». Une généralisation de telles techniques sera indispensable pour que l'ordinateur quantique puisse un jour réellement calculer.

Il faudra aussi augmenter le nombre d'ions. Comme la technique du couplage d'ions via leur mouvement sera d'autant plus difficile que la chaîne sera longue, d'autres techniques sont envisagées. Par exemple, l'équipe d'Innsbruck a proposé d'utiliser un ion piégé dans une tête mobile, portée par faisceau laser, qui peut interagir avec un ensemble d'ions immobiles dans un plan et transporter l'information quantique de qubit en qubit [8].

Le groupe du NIST propose, lui, de déplacer des ensembles d'ions entre des zones de calcul et des zones de stockage, en utilisant des électrodes miniaturisées. Ces idées présentent des similarités avec des concepts déjà utilisés en informatique, et des recherches impliquant des physiciens, des informaticiens et des ingénieurs ont été lancées en Europe et aux États-Unis afin de parvenir à la fois à miniaturiser les pièges et à augmenter le nombre d'ions piégés.

Combien de temps les ions piégés resteront-ils les meilleurs candidats qubits ? Parmi leurs avantages principaux figure l'efficacité de leur préparation et de leur lecture, ces manipulations s'effectuant pratiquement sans erreur. S'y ajoute un « temps de cohérence » assez long pour pouvoir effectuer un grand nombre d'opérations élémentaires (potentiellement plusieurs milliers). En revanche, le taux d'erreurs d'une porte logique individuelle devra être amélioré d'un facteur au moins 100

Un « abysse quantique » sépare un système accessible d'un ordinateur quantique

pour que l'ordinateur quantique puisse fonctionner – ce qui est difficile, mais pas inaccessible. Côté inconvénient, il faut noter la lenteur de l'opération d'une telle porte logique (10 000 fois plus lente que dans un micro-ordinateur). Sans compter que la gestion « qubit par qubit » de mémoires quantiques de grande taille est loin d'être évidente. Les calculs d'architecture montrent qu'un ordinateur quantique passe-

rait plus de 99 % de ses ressources à gérer sa mémoire et à corriger ses erreurs. Seulement 1 % servirait à effectuer le calcul proprement dit. Néanmoins, même avec ce problème, il conserverait l'avantage sur son cousin classique.

Les objectifs visés à cinq ou dix ans sont de réaliser des micropièges de 30 ions à 50 ions. Ces dispositifs seront capables de simuler des systèmes quantiques en interaction et, donc, de prédire leur évolution, déjà trop complexe pour être cal-

culée sur un ordinateur conventionnel.

Mais la factorisation d'un grand nombre est beaucoup plus exigeante. Par exemple,

le temps de calcul d'un ordinateur classique pour factoriser 2^{999} , codé avec 1 000 bits, est estimé de l'ordre du million d'années. Un ordinateur quantique pourrait effectuer ce même calcul beaucoup plus rapidement, mais il devra contenir plusieurs centaines de milliers de qubits.

Pour Wineland, un « abysse quantique » sépare un système a priori accessible (100 qubits) d'un ordinateur quantique « universel » (1 000 000 qubits). Ce défi est effectivement colossal. Pourtant, à l'heure actuelle, aucune objection physique fondamentale, qui interdirait par principe de réaliser un ordinateur quantique, n'a été énoncée. La gageure est donc purement technologique. Mais il reste très difficile de prédire si l'ordinateur quantique calculera un jour et, si c'est le cas, à quoi il ressemblera. Il semble néanmoins établi que les concepts qu'il utilisera, en particulier l'intrication, donneront accès à des idées physiques et à des perspectives d'applications radicalement nouvelles, dont les développements ne font sans doute que commencer. ■ F. S.-K. et Ph. G.

Cet article est la version revue et mise à jour par ses auteurs du texte paru dans le n° 398 de *La Recherche*.

CE DISPOSITIF INTÉGRÉ À ÉLECTRODES MULTIPLES a été conçu à l'université d'Ulm pour piéger et manipuler des ions individuels. C'est l'un des plus évolués pour déplacer les ions entre une « zone mémoire » et une « zone de calcul », comme dans un microprocesseur électronique.

