

Grover, des Laboratoires *Bell*. Avec un algorithme classique, la recherche d'un élément dans un ensemble de n objets exige en moyenne $n/2$ tentatives. Étonnamment, l'algorithme de L. Grover localise l'objet en $\sqrt{n}$ tentatives environ. Nous avons illustré ce gain de temps avec notre ordinateur quantique à deux bits, qui retrouve en une seule étape un objet, dans une liste de quatre objets. L'approche classique revient à ouvrir un cadenas à deux bits (à deux chiffres, chacun étant 0 ou 1) : on trouve très rarement la bonne combinaison du premier coup ; en moyenne il faut deux à trois tentatives.

Une limitation fondamentale de l'ordinateur à chloroforme est son petit

nombre de qubits. On pourrait augmenter ce nombre, mais n ne peut être plus grand que le nombre d'atomes de la molécule utilisée. Avec les dispositifs de RMN actuels, les plus gros ordinateurs quantiques manipuleraient seulement une dizaine de qubits (parce que, à température ambiante, l'intensité du signal désiré décroît rapidement à mesure que le nombre de noyaux magnétiques de la molécule augmente). Un équipement de RMN particulier, construit pour une molécule bien adaptée, multiplierait probablement ce nombre par trois ou par quatre.

Pour créer des ordinateurs encore plus gros, il faudrait recourir à d'autres techniques, comme le pompage optique, pour «refroidir» les spins : la

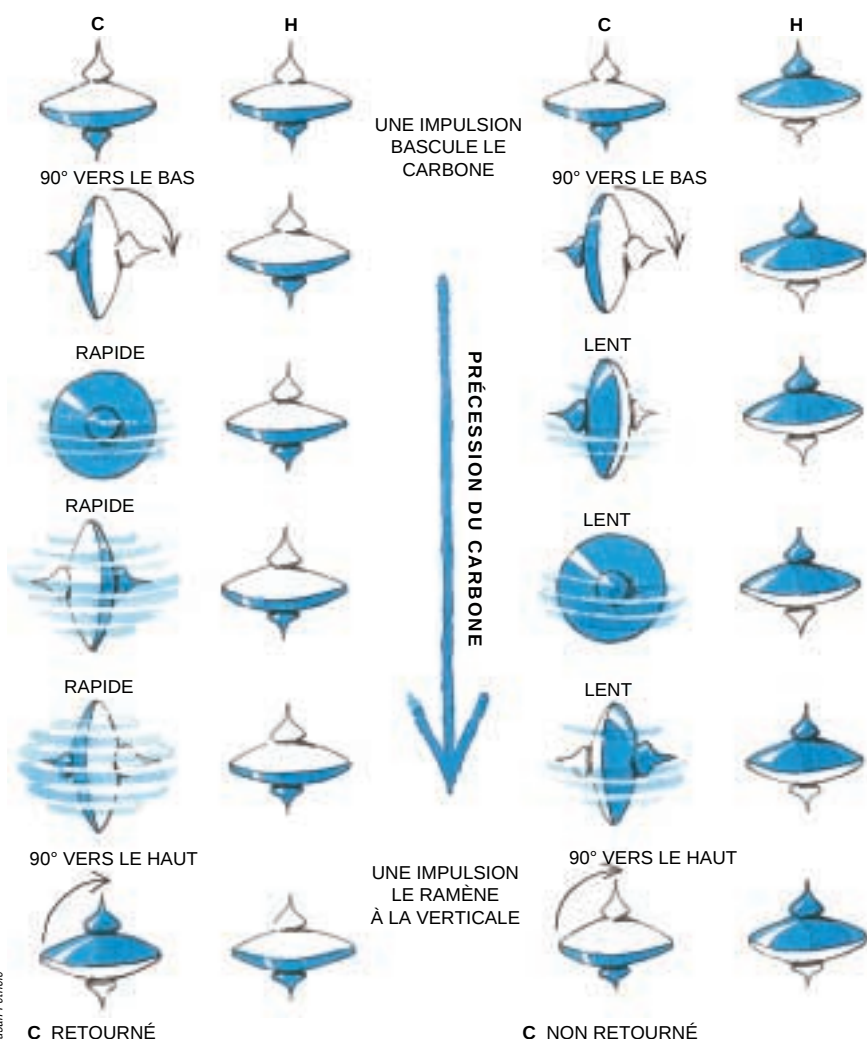
lumière émise par un laser orienterait presque tous les noyaux dans un même sens, sans qu'on ait besoin de geler le liquide (ce qui détruirait les grands temps de cohérence entre molécules).

La construction d'ordinateurs quantiques plus gros ne semble donc pas insurmontable. Quelle serait leur rapidité ? La durée d'un cycle dans un ordinateur quantique est déterminée par la plus petite vitesse d'inversion des spins. Celle-ci dépend à son tour des interactions entre les spins ; elle est généralement comprise entre quelques hertz et quelques centaines de hertz. Cela paraît très lent par rapport aux mégahertz (millions de cycles par seconde) atteints par les ordinateurs classiques. Pourtant, un ordinateur quantique disposant de suffisamment de qubits présenterait un tel parallélisme qu'il factoriserait un nombre de 400 chiffres en une année environ.

Perspectives

Comment le construire, concrètement ? Trouver des molécules contenant suffisamment d'atomes ne pose pas de difficultés, mais, lorsque la taille des molécules augmente, les interactions entre les spins les plus distants deviennent trop faibles pour être utilisées comme portes logiques. Pourtant, tout n'est pas perdu : Seth Lloyd, de l'Institut de technologie du Massachusetts, a montré que l'on pouvait en théorie construire de puissants ordinateurs quantiques, même si chaque atome n'interagit qu'avec ses plus proches voisins, à la manière des ordinateurs parallèles actuels. Ces ordinateurs quantiques pourraient utiliser de longues molécules hydrocarbonées et les techniques de la RMN. Les spins des nombreux noyaux atomiques, liés entre eux en longues chaînes, serviraient de qubits.

Un autre obstacle au calcul par RMN est la cohérence. Comme des nageurs synchronisés qui évolueraient sans repères, les noyaux d'un liquide perdent leur cohérence au bout de quelques secondes à quelques minutes, et les signaux de RMN qu'ils émettent se brouillent. Les plus grands temps de cohérence connus pour les fluides, comparés aux temps de cycle caractéristiques, suggèrent que les ordinateurs quantiques pourraient effectuer environ un millier d'opérations avant de perdre leur cohérence. Par chance, on peut repousser cette limite par l'ajout de



Dusan Petric

4. UNE PORTE LOGIQUE «NON CONTRÔLÉ» inverse l'une des deux entrées en fonction de l'état de la seconde entrée. Les auteurs ont fabriqué une porte «NON contrôlé» quantique en utilisant l'interaction entre les spins nucléaires de l'hydrogène et du carbone des molécules de chloroforme. Premièrement, une impulsion oscillante fait pivoter le noyau de carbone de 90 degrés. Ce noyau s'anime alors d'un mouvement de précession, qui est un peu plus rapide si l'hydrogène adjacent est dans un état que s'il est dans l'état opposé (sur la figure, on a noté «rapide» et «lent» pour simplifier). Après un laps de temps précis, une autre impulsion «90 degrés» provoque l'inversion du carbone (à gauche) ou le ramène dans sa position initiale (à droite), selon l'état de l'hydrogène voisin.

CADENAS CLASSIQUE



CONDITIONS INITIALES ALÉATOIRES



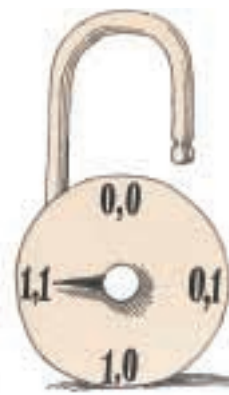
ON SE PLACE SUR LA PREMIÈRE COMBINAISON



PUIS ON ESSAIE LA SUIVANTE



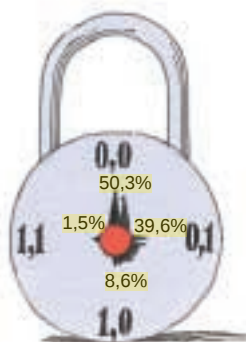
ET AINSI DE SUITE ...



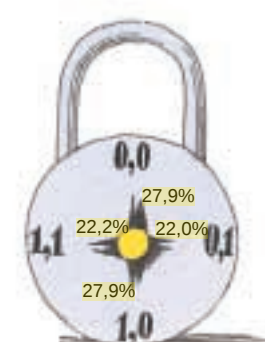
JUSQU'À CE QUE LE CADENAS S'OUVRE

Dusan Petric

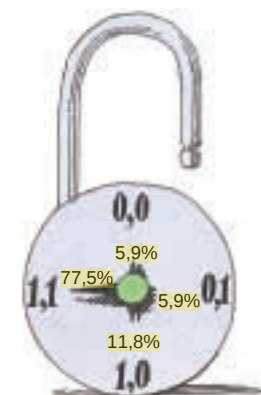
CADENAS QUANTIQUE



CONDITIONS INITIALES ALÉATOIRES



ON PRÉPARE LE CADENAS DANS LES QUATRE ÉTATS À LA FOIS



L'ALGORITHME DE GROVER DISTINGUE LE BON ÉTAT

← PHASE DE PRÉPARATION →

5. AVEC UN PEU DE MAGIE QUANTIQUE, on ouvre plus rapidement un cadenas. Par exemple, ouvrir un cadenas classique à deux bits peut demander jusqu'à quatre tentatives (en haut). En moyenne, un cadenas à n bits, qui a $N = 2^n$ combinaisons possibles, exige $N/2$ tentatives. Un cadenas quantique, en revanche, peut être placé simultanément dans de multiples états ; l'algorithme de Grover réduit alors le nombre de tentatives à environ $\sqrt{N}$. L'expérience réalisée par les auteurs (illustrée en bas) correspond à l'ouverture d'un cadenas quantique à deux bits. Après avoir été convenablement préparé, le cadenas livre sa combinaison dès la première tentative. Les pourcentages inscrits sur le cadenas indiquent les populations relatives mesurées pour chacun des quatre états quantiques.

qubits qui corrigeraient les erreurs quantiques.

Bien que les ordinateurs classiques utilisent des bits supplémentaires pour détecter et corriger les erreurs, nombre de spécialistes ont été surpris lorsque P. Shor et d'autres chercheurs montrèrent que l'on pouvait faire de même avec les ordinateurs quantiques. Ils pensaient que la correction d'erreurs quantiques imposerait de mesurer l'état du système et donc de détruire sa cohérence quantique. Il apparaît que l'on peut corriger les erreurs quantiques à l'intérieur de l'ordinateur sans que l'opérateur ait à lire les états responsables (voir l'article de Jean-Paul Delahaye, page 66, pour plus de détails).

La construction d'ordinateurs quantiques suffisamment gros pour rivaliser avec les plus rapides des ordinateurs classiques sera particulièrement difficile, mais les enjeux sont considérables : même les plus modestes ordinateurs quantiques constitueront de superbes laboratoires

d'analyse des principes de la théorie quantique.

Paradoxalement, ces ordinateurs quantiques pourraient résoudre les problèmes inhérents aux puces électroniques, dont les minuscules transistors se comportent de manière quantique lorsqu'on réduit leur taille jusqu'aux échelles atomiques.

Les ordinateurs classiques ne résolvent que très péniblement ces problèmes, qui seraient probablement très

simples pour les ordinateurs quantiques, comme l'envisageait Richard Feynman dès 1982.

Un point très encourageant est que ces ordinateurs n'exigeront pas de minuscules circuits à l'échelle atomique : la nature a déjà fait le plus gros du travail en assemblant les composants de base. Les molécules effectuent elles-mêmes des calculs remarquables. Seulement, on ne leur avait jamais posé les bonnes questions.

Neil GERSHENFELD est professeur à l'Institut de technologie du Massachusetts. Isaac CHUANG travaille au Centre de recherche d'IBM à San Jose (Californie).

Charles SLICHTER, *Principles of Magnetic Resonance*, troisième édition, Springer-Verlag, 1992.

Charles BENNETT, *Quantum Information and Computation*, in *Physics Today*, vol. 48, n° 10, pp. 24-30, octobre 1995.

Seth LLOYD, *Les ordinateurs quantiques*,

Pour la Science, n° 218, pp. 44-50, déc. 1995.

Neil GERSHENFELD et Isaac CHUANG, *Bulk Spin-Resonance Quantum Computation*, in *Science*, vol. 275, pp. 350-356, 17 janvier 1997.

Lov GROVER, *Quantum Mechanics Helps in Searching for a Needle in a Haystack*, in *Physical Review Letters*, vol. 79, n° 2, pp. 325-328, 14 juillet 1997.

Jean-Paul DELAHAYE, *Les ordinateurs quantiques*, *Pour la Science*, vol. 209, pp. 100-104, mars 1995.