sique. Peter Shor remarqua qu'on peut détecter une erreur et la corriger sans avoir à en prendre connaissance en détail.

La méthode de Peter Shor a été généralisée et étendue aux diverses sources d'erreurs qu'on rencontre lors du déroulement d'un calcul quantique. Après trois ans de travaux, les chercheurs en sont arrivés à la conclusion ferme que, non seulement on peut corriger les erreurs, mais qu'on peut préserver un état quantique complexe et le manipuler pendant des intervalles de temps aussi longs qu'on le souhaite, avec un risque global d'erreur aussi petit qu'on le désire. Précisons toutefois qu'il s'agit d'une avancée théorique qui n'a pas aujourd'hui été expérimentalement mise en œuvre, ce qui demandera sans doute de nombreuses années.

L'intérêt de la superposition quantique et du calcul quantique est soumis à une objection grave fondée sur l'impossibilité de connaître complètement certains états quantiques : à quoi peut bien servir d'engendrer un état quantique contenant la superposition de f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1), si l'on ne peut pas en extraire – ce qui est le cas – la connaissance de f(0,0,0)?

L'algorithmique quantique

Cette question est très gênante. La réponse n'est devenue claire que progressivement, par le développement d'algorithmes quantiques délicats qui exploitent astucieusement les superpositions d'états et les opérations que la théorie quantique autorise sur eux pour extraire des superpositions des informations utiles. Le premier résultat important (dû à Peter Shor en avril 1994) est un algorithme rapide pour la factorisation des nombres entiers. Comme aucun algorithme rapide classique n'existe, cette découverte créa un certain émoi chez les spécialistes et suscita une vague d'intérêt pour les ordinateurs quantiques (sauf en France, où l'on préféra se spécialiser dans l'explication de l'impossibilité à surmonter la décohérence).

Le second problème algorithmique important traité fut celui du repérage d'une donnée dans une liste non organisée par Lov Grover *(voir l'article de N. Gershenfeld et I. Chuang dans ce numéro)*. Cet algorithme est plus important encore que le premier car ses applications potentielles touchent cette fois non seulement la cryptographie, mais aussi le traitement général des données, quelle qu'en soit la nature.

Des résultats récents montrent aussi – comme on pouvait le présumer – qu'un ordinateur quantique n'aurait pas d'équivalent pour étudier les systèmes quantiques quelconques et qu'il permettrait de les simuler avec efficacité, ce qui est impossible avec un ordinateur classique.

D'autres algorithmes plus spécialisés sont proposés régulièrement et on commence à comprendre ce nouvel art de programmer que nécessiteront les ordinateurs quantiques. Cet ensemble de résultats a une incidence sur les fondements de la théorie du calcul, car il remet en cause une de ses bases : l'acceptation que tous les mécanismes de calcul sont sensiblement équivalents en puissance (en langage précis : que chacun est simulable en temps polynomial par chaque autre). La première victime de ce bouleversement est dès

LA TÉLÉPORTATION SERA-T-ELLE QUANTIQUE?

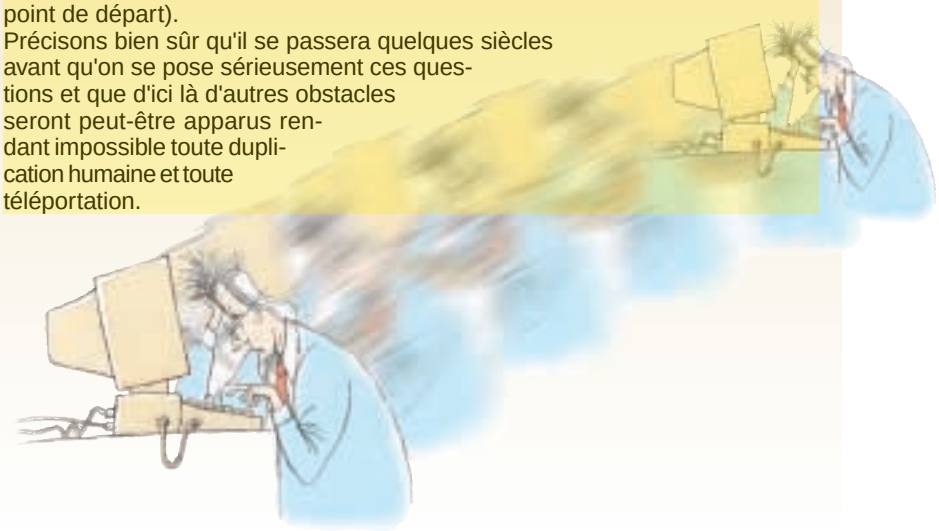
Si l'on pense qu'une personne humaine n'est pas seulement définie par l'état physique de son corps et de son cerveau (question philosophique) alors aucune discussion n'est possible. Supposons donc que l'intégrité d'une personne humaine n'est qu'une question physique. Deux cas apparaissent.

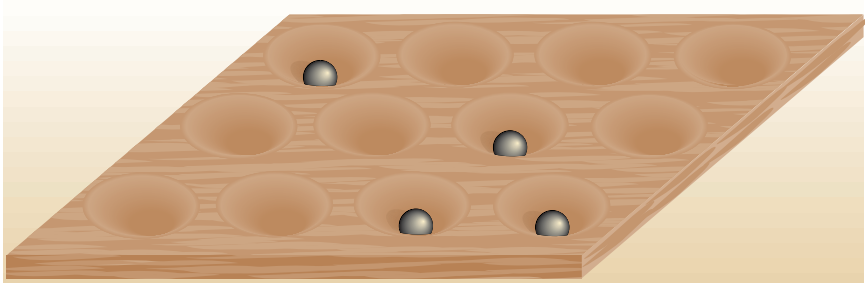
Cas 1. La mécanique quantique ne joue pas de rôle essentiel dans le fonctionnement du corps et du cerveau. En prenant connaissance à un niveau de détail assez fin de la position des atomes qui composent le voyageur (chose peut-être impossible mais qu'aujourd'hui aucun principe n'interdit) on pourrait transmettre cette information d'un point à un autre (par radio) et mener au point d'arrivée une reconstruction du voyageur. Dans un tel cas la téléportation fait voyager à la vitesse de la lumière. Les hypothèses mises en œuvre ici permettent en théorie de dupliquer une personne humaine (après avoir pris connaissance de sa définition on en reconstitue plusieurs copies), comme dans certains épisodes de Star Trek lorsque l'appareil de téléportation fonctionne mal.

La quantité d'information impliquée dans ces opérations est parfois évoquée pour dire qu'aucun canal d'information n'aura jamais assez de puissance pour transmettre l'information nécessaire qui serait au moins de 10^{30} bits. Cet argument néglige les possibilités de compression d'information : pour transmettre l'information décrivant un corps humain il n'est pas nécessaire par exemple de transmettre la description des chromosomes de chaque cellule puisque dans chacune des milliards de cellules d'un organisme vivant ce sont les mêmes chromosomes qu'on trouve.

Cas 2. La mécanique quantique joue un rôle essentiel dans le fonctionnement du corps et du cerveau qui utilise peut-être des atomes corrélés et des superpositions complexes d'états quantiques pour fonctionner. Aucune mesure complète de l'état instantané du voyageur ne sera possible et donc sa duplication sera impossible. En revanche, la technique de téléportation quantique s'appliquerait et produirait le déplacement à la vitesse de la lumière (mais pas plus, là encore) d'un voyageur (qui serait alors nécessairement détruit à son point de départ).

Précisons bien sûr qu'il se passera quelques siècles avant qu'on se pose sérieusement ces questions et que d'ici là d'autres obstacles seront peut-être apparus rendant impossible toute duplication humaine et toute téléportation.





4. LA DISCRÉTISATION. Quiconque calcule avec des billes pour se repérer (comme on le faisait autrefois quand on calculait avec des jetons) n'a pas besoin, à chaque déplacement de bille, de la poser au centre du trou visé. De légères erreurs lors des déplacements se corrigent automatiquement du seul fait de la forme de la surface, qui rectifie les écarts modérés. Ce passage du plan continu à une surface autocorrectrice à trous est analogue à l'introduction des codes correcteurs d'erreur dans les ordinateurs. Ces codes transforment un ensemble de positions infini (difficile à contrôler lors de longues séquences d'opérations), en un ensemble fini de positions. C'est la discrétisation de l'espace d'états. Ces codes correcteurs qui réduisent l'espace d'états de l'ordinateur, correspondent physiquement à un refroidissement du système et produisent donc une dissipation de chaleur. Dans le cas des ordinateurs quantiques — qui en théorie fonctionnent de manière réversible, donc sans dissipation — les codes correcteurs d'erreur seraient le dispositif consommateur d'énergie.

aujourd'hui la cryptographie mathématique, qui se voit mise en concurrence avec la cryptographie quantique et qui, si l'on progresse dans la réalisation concrète des ordinateurs quantiques, devra être revue de fond en comble à cause des algorithmes de P. Shor et de L. Grover.

La théorie de la transmission d'informations de Claude Shannon, qui est essentiellement classique, a été ajustée au cas quantique ; des résultats particuliers concernant la compression de l'information quantique ont été proposés. Tout cela, ajouté à la nouvelle algorithmique, constitue maintenant un ensemble théorique puissant, une nouvelle discipline à l'intersection de l'informatique et de la physique. Cette nouvelle discipline est la véritable informatique théorique et s'oppose à l'informatique théorique classique, fondée sur une conception en partie erronée de l'information et du calcul qui néglige la réalité physique de notre Univers. Pour Andrew Steane, «Le fait que la théorie classique de l'information s'adapte à la mécanique quantique comme une main dans un gant et la surprenante cohérence générale de la nouvelle discipline donnent l'impression que nous accédons à des vérités profondes de la nature.»

Concernant l'informatique quantique le scepticisme est une attitude raisonnable, mais il semble non moins raisonnable de proclamer, avec J. Preskill, que «la construction d'ordinateurs quantiques est un rêve qui pourrait changer le monde, aussi laissez-nous rêver.»

Jean-Paul DELAHAYE est professeur d'informatique à l'Université de Lille.

J. PRESKILL, *Course Information for Physics 229, Advanced Mathematical Methods of Physics*, California Institute of Technology, Pasadena. Remarquables notes d'un cours donné en 1997-1998. Disponible à l'adresse Internet : http://www.theory.caltech.edu/people/preskill/ph2

Andrew STEANE, *Quantum Computing. 1997*. Notes disponibles à la même adresse que le précédent cours.

C. BENNETT, G. BRASSARD, C. CRÉPEAU, R. JOZSA, A. PERES et W. WOOTTERS, *Teleporting an Unknown Quantum State ...*, in *Physical Review Letters*, 29 mars 1993, vol. 70, n°13, pp. 1895-1899.

I. CHUANG, N. GERSHENFELD et M. KUBINEC, *Experimental Implementation of Fast Quantum Searching*, in *Physical Review Letter* (à paraître).

J.-P. DELAHAYE, *Les ordinateurs quantiques*, in *Pour La Science*, n° 209, 100-105, mars 1995.

L. K. GROVER, *A Fast Quantum Mechanical Algorithm ...*, in *Proceedings of the 28th Annual Symposium on the Theory of Computing. STOC*, pp. 212-219, 1996,

P. SHOR, *Polynomial-time Algorithms for Prime Factorization and Dicrete Logarithm on a Quantum Computer*, in *Proc. of the 35th Annual Symposium. on Foundations of Computer Science, Santa Fe*, IEEE Computer Society Press, pp. 124-139, 1994.