Zeitschrift: Tracés : bulletin technique de la Suisse romande
Herausgeber: Société suisse des ingénieurs et des architectes
Band: 130 (2004)
Heft: 13: Ordinateur quantique

Artikel: Les lois étranges de l'information quantique
Autor: Delahaye, Jean-Paul
DOI: https://doi.org/10.5169/seals-99322

Jean-Paul Delahaye

Les **lois étranges** de l'information quantique

Ce qui semble aller de soi, en physique classique, est erroné dans un monde régi par la mécanique quantique, où la définition et la pratique du calcul changent et remettent en cause les fondements de l'informatique théorique. Principe de non-duplication, téléportation, phénomène de la mesure qui change l'objet mesuré : ces propriétés déconcertantes autorisent cependant - si elles sont utilisées avec astuce - des manipulations et des calculs impossibles jusqu'alors.

La mécanique quantique propose une conception des objets physiques difficile à concilier avec celle - classique - que nous tirons de nos expériences au niveau macroscopique. Un système quantique, par exemple, peut se trouver dans un état de superposition[1] : c'est comme si la lampe devant vous n'était ni éteinte ni allumée, mais se trouvait dans un état réunissant les deux possibilités... et tous les états intermédiaires (fig. 1). Tout aussi inattendue, l'information - dont on croyait à tort qu'elle n'était qu'un concept mathématique indépendant de la physique - doit être envisagée avec un œil nouveau pour tenir compte de ce que les physiciens ont découvert du monde quantique. C'est une véritable révolution : si le monde est régi par la mécanique quantique - ce que l'on a de bonnes raisons de croire - alors la manipulation de l'information est soumise à des lois bien différentes de celles de l'information dans un monde classique. Il nous faut apprendre à penser d'une façon nouvelle, mais le jeu en vaut la chandelle, car les théoriciens ont montré que l'utilisation judicieuse des propriétés quantiques de l'information peut faire des miracles. Acquérir de l'information, la copier, la cacher, la mémoriser, la combiner etc. - tout cela se déroule autrement dans le monde quantique et remet en cause les fondements même de l'informatique. Naît alors le rêve d'un ordinateur quantique surpassant tout ordinateur classique.

Le lecteur modifie le livre

Dans le monde classique, lire un livre n'en change pas le texte. Dans le monde classique, l'information est une dimension abstraite. Un objet est le même, peu importe si l'on en a connaissance. Acquérir de l'information à propos de certains systèmes quantiques, en revanche, les perturbe irrémédiablement. C'est là une conséquence du principe d'indétermination d'Heisenberg : s'intéresser à une grandeur mesurable d'un objet interdit d'en connaître d'autres et, plus précisément, en fait un autre objet[2].

La chose est manifeste lorsque, face à un photon (c'est-à-dire un grain de lumière), on cherche à en connaître la direction de polarisation : cela n'est possible que partiellement et en le perturbant. Par exemple, si l'on dispose d'un photon qui se propage selon une direction de polarisation caractérisée par un angle α, aucune mesure ne peut déterminer α entièrement. Sans informations préalables, la polarisation est impossible à connaître, car l'opération de mesure - ici le passage à travers un filtre - détruit l'état quantique du photon étudié (fig. 2).

Indéterminisme et non-duplication

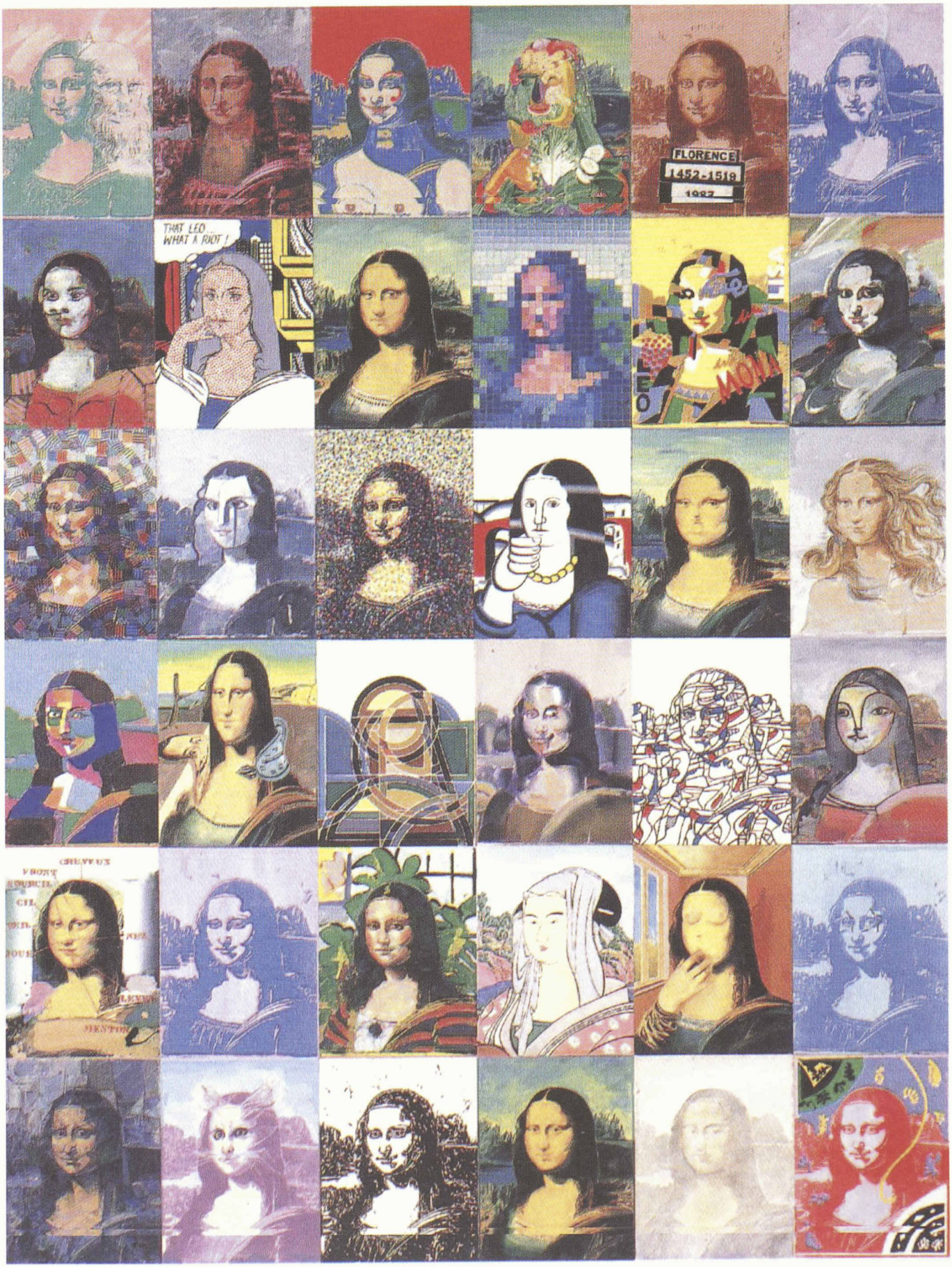
C'est également le photon qui montre que l'information quantique est parfois authentiquement aléatoire : si, après avoir polarisé un photon selon une direction α, on le fait passer par un filtre polarisant dont l'axe fait un angle de 45° avec α, on le détectera une fois sur deux exactement. En

[1] La plupart des aspects du monde quantique qui vont à l'encontre du sens commun proviennent du principe de superposition, selon lequel il est possible de décrire, par exemple, une particule localisée, au même instant, en deux positions différentes. Ce phénomène est la règle à l'échelle microscopique, même s'il est difficile de se le représenter : on n'observe jamais de superpositions quantiques à l'échelle macroscopique. Dans un article célèbre de 1935, Erwin Schrödinger donne, en quelques lignes, une illustration frappante de cet apparent paradoxe (voir, entre autres, Erwin Schrödinger : « Physique quantique et représentation du monde », *Seuil*, Points sciences, 1992).

[2] Werner Heisenberg, Prix Nobel de physique en 1932, est l'un des principaux fondateurs de la mécanique quantique. Il montre que, pour des phénomènes ayant lieu à l'échelle atomique, toute tentative visant à déterminer une valeur d'un système donné a pour conséquence de perturber d'une façon imprévisible d'autres grandeurs de ce système.

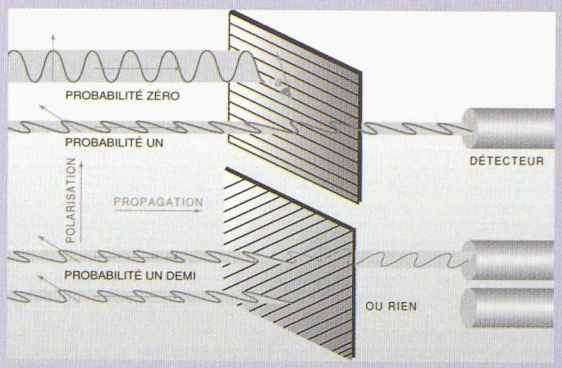
Fig. 1 : Les multiples états d'âme de Mona Lisa : une sorte de portrait de son état quantique
(Document Faculté de philosophie de l'Université de Brno, République tchèque)

Fig. 2 : L'opération de mesure détruit l'état quantique du photon.
(Document Pour la science*)*



1

Un photon se propage selon une direction de polarisation perpendiculaire à son axe de propagation. Cette direction est caractérisée par un angle α (entre 0 et 180°), qu'aucune mesure ne peut déterminer entièrement. Si, pour tenter de connaître cet angle, on place sur le trajet du photon un filtre polarisant d'angle 0, suivi d'un détecteur, alors le photon passera certainement si $\alpha = 0$, et sera intercepté si $\alpha = 90°$. Il passera avec une probabilité de $\cos^2\alpha$ pour les angles intermédiaires. La détection ou non du photon est donc insuffisante pour identifier l'angle α. Plus grave, en passant par le filtre polarisant, le photon perd son orientation primitive, ce qui rend l'angle α définitivement inconnaissable et le photon impossible à dupliquer (« no-cloning principle »). Si l'on fait passer par le dispositif une suite de photons ayant chacun un angle de polarisation $\alpha = 45°$, la probabilité pour chaque photon d'être détecté après passage par le filtre est exactement 1/2. La suite des résultats (« 1 » pour interception, « 0 » pour non-détection) possède toutes les propriétés attendues d'une suite aléatoire de 0 et de 1.



2

reproduisant l'expérience, la suite obtenue de 1 et de 0 (« 1 » pour une détection ; « 0 » pour une absence de détection) possédera les propriétés d'une suite générée par une variable aléatoire mathématique parfaite. C'est dire que l'aléatoire est au cœur de la mécanique quantique. On construit d'ailleurs des générateurs de bits aléatoires fondés sur des mécanismes quantiques, et la société suisse *id Quantique* vend un tel générateur depuis quelques mois (voir aussi p. 20).

Les moines du Moyen âge, nos photocopieuses, nos ordinateurs copient des informations sans jamais rencontrer d'obstacles fondamentaux. Si une information classique est disponible, en faire de multiples versions est facile et ne coûte presque rien (sauf aux éditeurs de livres et de musique...). Dans le monde classique, l'information est copiable. Dans le monde quantique, on rencontre des cas où la copie n'est pas possible. Le principe de non-duplication (« no-cloning principle ») énoncé par W. Wootters, W. Zurek et D. Dieks en 1982 exprime cette impossibilité fondamentale : un état quantique inconnu ne peut pas être dupliqué.

Reprenons notre photon : vous ne réussirez jamais à le dupliquer si vous n'en savez rien, car vous ne pourrez jamais connaître complètement son état quantique. Si vous essayez, dès que vous commencez à mesurer certaines observables (la polarisation selon une direction α par exemple), vous en détruirez l'état quantique et serez donc incapable de connaître d'autres observables. La duplication du photon est impossible. Notons toutefois que lorsqu'une information est connue, comme dans le monde classique, on peut la reproduire.

Une information non-localisée

Cacher de l'information classique - ce qui est le but de la cryptographie - semble difficile, du moins la cacher de façon mathématiquement garantie. En revanche, la cryptographie quantique fondée sur le principe de non-duplication des photons quantiques propose des méthodes de distribution de clefs secrètes qui sont sûres et n'ont aucun équivalent classique (voir aussi pp. 20 à 22).

La plus singulière propriété de l'information quantique est cependant la non-localité : une information quantique ne se situe pas nécessairement en un endroit précis. Dans certaines circonstances, l'information quantique est étalée dans l'espace entier. John Bell a établi en 1964 que les prédictions de la mécanique quantique ne peuvent être reproduites par aucune théorie à variables cachées locales (théorie où chaque information est située en un point précis de l'espace). Les prédictions résultant de son analyse furent vérifiées par Alain Aspect et son équipe en 1982. En montrant ainsi que de l'information s'étale entre diverses parties éloignées d'un système physique (chose qui par définition est exclue du modèle général des ordinateurs classiques où, à chaque instant, chaque information est localisée), Bell a rendu vraisemblables les nouvelles possibilités de traitement de l'information offertes par la théorie quantique.

La téléportation quantique est un exemple de ces possibilités nouvelles inattendues : déplacer à la vitesse de la lumière une information inconnue sans en prendre connaissance semblait impossible. Or cela est réalisable. Cette technique - dont le principe a été proposé en 1993 par C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Perez et W. Wootters - fait voyager à la vitesse de la lumière un état quantique inconnu. Depuis, de nombreuses équipes ont vérifié expérimentalement l'analyse théorique en téléportant à la vitesse de la lumière des informations inconnues.

La capacité supérieure du calcul quantique fut clairement pressentie dès 1982 par le Prix Nobel Richard Feynman, puis mise en évidence dans un cas (théorique) précis en 1985 par David Deutsch. Les développements de l'algorithmique quantique et les expériences de calcul quantique de ces dernières années montrent que les prévisions des modèles théoriques ne sont pas des chimères et que, lorsqu'on se fixe le but de mener des calculs, les propriétés étranges de l'information quantique sont utiles et engendrent des miracles. Pour expliquer cela nous devons évoquer le qubit.

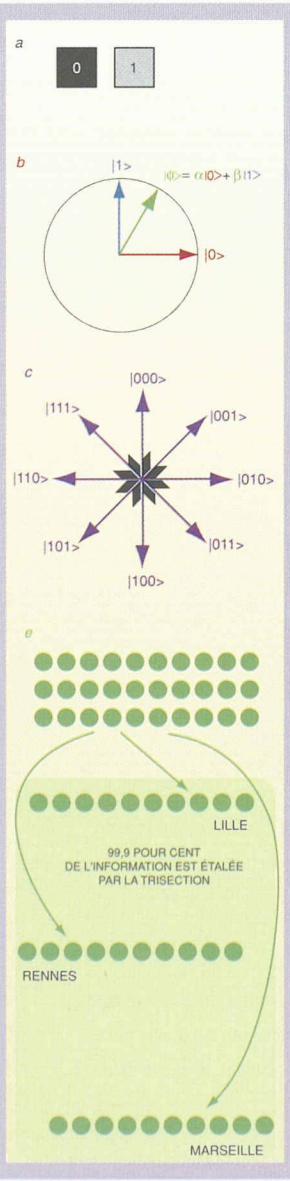
L'information et son support

Le support élémentaire de l'information classique est le bit : un 0 ou un 1. Son analogue quantique est le qubit, le *quantum bit*. En théorie, n'importe quel système matériel pouvant se trouver dans deux états différents représente un bit ou un qubit : un curseur tourné vers la droite ou vers la gauche ; un espace convenu sur un papier qu'on noircit ou non ; le spin d'un noyau d'atome orienté vers le haut ou vers le bas, etc. Cependant, les principes de la mécanique quantique qui autorisent la superposition d'états font du qubit un outil de mémorisation et de calcul incomparablement plus puissant que le bit.

Fig. 3 : Propriétés de l'informatique quantique (Document Pour la science*)*

Un qubit dans un état $\alpha|0> + \beta|1>$ (un peu de 0, en même temps qu'un peu de 1) code bien plus d'informations qu'un bit classique. Un N-qubit demande, pour être décrit complètement, non pas qu'on indique N choix entre 0 ou 1 (cas classique), mais qu'on spécifie 2^N choix de nombres complexes (fig. 3). Avec un même qubit, par superposition, on mémorise en quelque sorte non pas « 0 ou 1 » mais « 0 et 1 avec les proportions de 0 et de 1 ». Avec un 2-qubit on mémorise simultanément quatre états différents. Avec un 10-qubit on mémorise un millier d'états (2^{10}) et avec un 30-qubit on atteint le milliard (2^{30}).

Calculer avec des qubits revient à faire simultanément plusieurs calculs à la fois (on parle de parallélisme quantique) : avec un 3-qubit, on calculera la valeur d'une fonction en même temps pour les huit jeux de données : (0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1). Pour dire tout cela de manière imagée : grâce à la superposition quantique, tout se passe comme si, à partir d'un système de calcul, vous



a) Un bit

L'information unitaire classique est le bit : un objet qui vaut 0 ou 1.

b) Un qubit

L'information unitaire quantique est le qubit (*quantum bit*). C'est un vecteur dans un espace complexe de dimension 2 muni d'un produit scalaire (deux vecteurs dont le produit scalaire est nul sont orthogonaux). Les éléments d'une base orthogonale sont fixés et notés $|0>$ et $|1>$. Un qubit $|\phi>$ se représente sous la forme : $|\phi> = \alpha|0> + \beta|1>$ avec $|\alpha|^2 + |\beta|^2 = 1$, où α et β sont des nombres complexes (ainsi le qubit est déterminé par quatre nombres réels). Quand on procède à une mesure, cela ramène le qubit $|\phi>$ sur l'un des vecteurs de la base $|0>$, $|1>$. Le résultat n'est pas déterminé. Les règles de la mécanique quantique indiquent qu'on obtient, lors d'une mesure physique : $|0>$ avec la probabilité $|\alpha|^2$ et $|1>$ avec la probabilité $|\beta|^2$

c) Un N-qubit

L'état quantique d'un N-qubit est un vecteur dans un espace analogue à celui du qubit, mais cette fois de dimension 2^N. On choisit une base orthogonale de cet espace correspondant aux vecteurs dont chaque composante a une valeur $|0>$ ou $|1>$. Pour un 3-qubit, on choisit une base orthogonale dont les vecteurs sont : $|000>$, $|001>$, $|010>$, $|011>$, $|100>$, $|101>$, $|110>$, $|111>$. Un état général du 3-qubit est alors de la forme : $a_{000}|000> + a_{001}|001> + a_{010}|010> + a_{011}|011> + a_{100}|100> + a_{101}|101> + a_{110}|110> + a_{111}|111>$ où les coefficients sont des nombres complexes vérifiant : $|a_{000}|^2+|a_{001}|^2+|a_{010}|^2+|a_{011}|^2+|a_{100}|^2+|a_{101}|^2+|a_{110}|^2+|a_{111}|^2 = 1$
En cas de lecture du 3-qubit, on obtient un vecteur de la base, chaque vecteur $|ijk>$ de la base étant obtenu avec une probabilité proportionnelle à $|a_{ijk}|^2$.

d) Le calcul quantique

Réaliser un calcul quantique consiste à préparer un N-qubit dans un état initial standard, par exemple $|00...0>$ puis à appliquer à cet état une série de transformations unitaires (ce sont des opérations analogues en dimension quelconque aux rotations d'un vecteur). A la fin de cette suite de transformations, on mesure le N-qubit par une expérience qui l'amène dans un état correspondant à un vecteur de la base orthogonale, ce qui donne par exemple $|001>$. Le résultat de cette mesure est probabiliste : on ne sait jamais ce que l'on va trouver. Tout l'art de la programmation quantique réside dans le choix des opérateurs qu'on applique de façon à ce qu'il se produise quelque chose d'intéressant (par exemple la factorisation d'un entier). Le plus souvent, un calcul quantique commence par la création d'une superposition homogène de tous les états de la base. Pour un 3-qubit, par exemple, on commence par créer : $[|000> + |001> + |010> + |011> + |100> + |101> + |110> + |111>]/\sqrt{8}$. On voit qu'un N-qubit est un objet difficile à décrire : il faut, pour le spécifier complètement, indiquer 2^N nombres complexes.
Nos ordinateurs actuels ne sont pas assez puissants pour contenir la description d'un 100-qubit, ni a fortiori pour simuler le calcul d'un ordinateur quantique ayant une mémoire de 100-qubit. Alors qu'en principe un calculateur quantique est toujours simulable par un calculateur classique, en pratique ce n'est pas le cas. Il n'était pas évident que les règles délicates du calcul quantique par transformations unitaires produisent quelque chose d'intéressant. C'est pourtant ce qu'ont montré Peter Shor, Lov Grover et les algorithmiciens quantiques.

e) La non-localité : un résultat de Don Page

« Moins d'un millième de l'information est localement accessible, les 999 autres millièmes sont dans le nuage central. »
La possibilité de coder des informations globalement dans un N-qubit est mise en évidence par l'exemple suivant : un de vos amis choisit un 30-qubit quelconque et en prépare un très grand nombre d'exemplaires (comme il l'a choisi lui-même, cela ne contredit pas le principe de non-duplication). En faisant une série assez longue de mesures sur les divers exemplaires du 30-qubit on peut en reconstituer l'état avec exactitude. Mais, au lieu de cela, on divise chaque 30-qubit en trois sous-ensembles de 10-qubit qu'on envoie à Rennes, Lille et Marseille. En faisant des mesures localement et indépendamment dans ces trois villes (c'est-à-dire sans coordonner ni corréler les mesures), on ne peut, d'après un résultat de Don Page, tirer en moyenne que moins d'un millième de l'information contenue dans le 30-qubit, et cela quel que soit le nombre de copies dont on dispose. L'information contenue dans le 30-qubit est intrinsèquement non locale, et seules des mesures collectives peuvent la révéler.

3

réussissiez à en avoir plusieurs par superposition, chacun travaillant de son côté. Ce qui bien sûr démultiplie la quantité de calculs effectués et rend votre système de calcul plus puissant.

Un obstacle fondamental à l'utilisation d'un N-qubit est cependant la décohérence, c'est-à-dire la propension d'un état quantique à interagir spontanément avec son environnement, ce qui - en projetant son état sur l'un des états de base - détruit son caractère multiple (et donc sa capacité à mener des calculs en parallèle). Cependant, depuis la fin des années 1990, on a conçu des méthodes de correction d'erreurs qui - en théorie - permettent de limiter ces instabilités et rendraient donc possible ce parallélisme miraculeux.

L'algorithmique quantique

A vrai dire, l'utilisation de la superposition quantique est soumise à une autre difficulté qui est basée sur l'impossibilité de connaître complètement certains états quantiques (ce que nous avons vu à propos du photon polarisé) : à quoi peut bien servir de générer un état quantique contenant la superposition des valeurs calculées 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) ? Le monde quantique semble calculer pour lui seul en parallèle, en refusant de livrer le résultat de ses calculs à l'observateur. Ce qu'on gagne d'un côté (par le parallélisme) serait donc perdu d'un autre (par l'impossibilité de connaître complètement l'état quantique d'un système) ?

La réponse n'est devenue claire que progressivement par le développement d'algorithmes quantiques qui exploitent les superpositions d'états et les opérations que la théorie quantique autorise, et qui réussissent finalement à en tirer des résultats utiles, le tout réalisant au bout du compte certaines opérations sans équivalent classique. Finalement - et ce ne fut pas évident à comprendre -, ce qu'on gagne d'un côté n'est pas perdu de l'autre. Bien au contraire : passer par le monde quantique se révèle formidablement payant.

Le premier résultat important - dû à Peter Shor en 1994 - est un algorithme quantique rapide pour la factorisation des nombres entiers (factoriser, c'est par exemple trouver que 143=11x13 ; 11 et 13 étant des nombres premiers). Le problème de la factorisation est central en cryptographie, et considéré comme intrinsèquement difficile. La découverte que le monde quantique autorisait la factorisation rapide des nombres entiers surprit les spécialistes et engendra une vague considérable d'intérêt pour les ordinateurs quantiques, intérêt qui n'est pas retombé depuis.

Le second problème algorithmique important traité fut celui du repérage d'une donnée dans une liste non organisée par Lov Grover. Cet algorithme (utile pour la classification de données ou pour certaines explorations combinatoires) est plus important encore que le premier, car ses applications possibles concernent non seulement la cryptographie, mais aussi le traitement général de l'information.

Un nouvel art

D'autres résultats montrent - comme on s'y attendait - qu'un ordinateur quantique n'aurait pas d'équivalent pour étudier et simuler efficacement les systèmes quantiques quelconques qu'il permettrait de simuler avec efficacité, chose impossible avec un ordinateur classique. Des algorithmes plus spécialisés sont proposés régulièrement et nous commençons à comprendre ce nouvel art de programmer nécessaire aux ordinateurs quantiques.

Aujourd'hui, la mise au point technique des ordinateurs quantiques (voir bibliographie) ne se fait que très lentement, et on considère comme un exploit d'avoir, en 2002, factorisé 15=3x5 à l'aide d'un calcul utilisant des 7-qubits. Cependant, nous savons que les promesses faites par les théoriciens dans le passé (concernant les effets de la non-localité, de la superposition ou la téléportation quantique, etc.) ont toujours fini par se traduire expérimentalement. Nous avons donc de bonnes raisons d'espérer que - même sous forme rudimentaire - les ordinateurs quantiques viennent supplanter pour certaines tâches nos bons vieux ordinateurs classiques.

Jean-Paul Delahaye
Professeur à l'Université des Sciences et Technologies de Lille
Laboratoire d'Informatique Fondamentale de Lille
UMR CNRS 8022, Bât. M3, F - 59655 Villeneuve d'Ascq Cedex

Bibliographie

[1] Dirk Bouwmeester, Artur Ekert, Anton Zeilinger (eds.) : « The Physics of Quantum Information », *Springer*, 2000 [ouvrage technique et très complet pour une introduction approfondie]

[2] Jean-Paul Delahaye : « L'intelligence et le calcul : de Gödel aux ordinateurs quantiques », Editions *Pour la science*, Berlin/Paris, 2002 [ouvrage de niveau technique moyen pour une introduction rapide]

[3] Tom Siegfried : « The bit and the Pendulum : From Quantum Computing to M Theory, The New Physics of Information », John Wiley and Sons, New York, 2000 [ouvrage non technique pour le grand public]