Les lois nouvelles de l'information quantique

JEAN-PAUL DELAHAYE

Principe de non-duplication, téléportation, cryptographie inviolable, codes correcteurs, parallélisme illimité : l'informatique quantique est née.

Quand, en 1937, George Stibitz fabrique dans sa cuisine un additionneur binaire à relais qui fonctionne avec deux chiffres (et qui ne fait donc que 4 additions différentes, 0+0, 0+1, 1+0 et 1+1), il ne suscite aucun enthousiasme. Quelques années plus tard, les descendants de sa machine, les ordinateurs, ont envahi le monde.

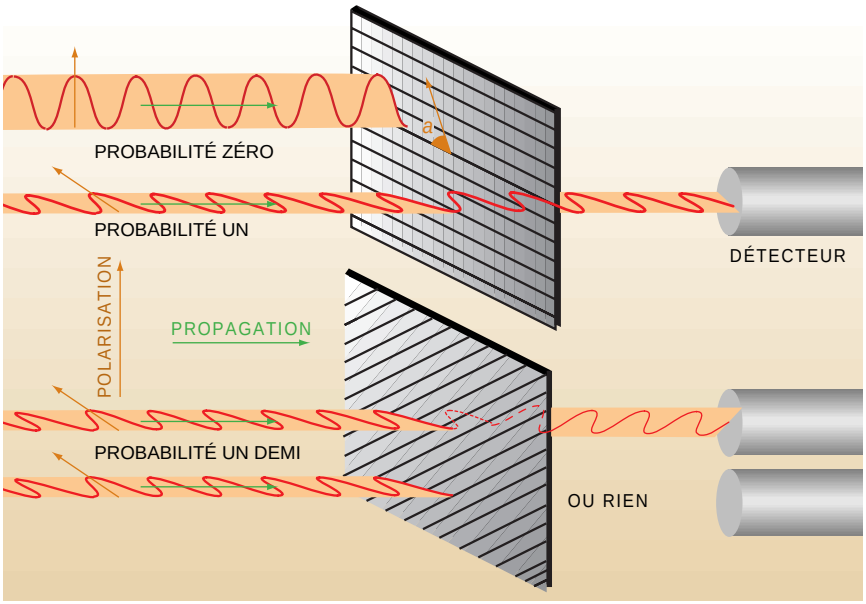
Les physiciens quantiques viennent de fabriquer l'équivalent quantique de l'additionneur de Stibitz et la théorie du calcul quantique prouve que, si l'on progresse normalement, les ordinateurs quantiques seront plus puissants que ne pourrait l'être un ordinateur classique de la taille du système solaire fonctionnant à la vitesse de la lumière avec des unités de mémoire de la taille de l'atome : nous vivons la naissance d'une technologie fondée sur les miracles théoriques du monde quantique, et qui projette ceux-ci dans notre réalité quotidienne.

Parallèlement à nos premiers pas vers ces calculateurs de rêve, une révolution modifie notre conception de l'information. Naïvement, nous avons trop longtemps adopté une vue préquantique de l'information. Pourtant ce qui «va de soi» concernant l'information est erroné si le monde est régi par la mécanique quantique. Le traitement de l'information dans un monde quantique est différent de sa manipulation dans un monde classique : il nous faut découvrir et pratiquer de nouvelles règles pour acquérir de l'information, la copier, la cacher, la mémoriser, la combiner, etc. En conséquence, la définition et la pratique du calcul changent et remettent en cause les fondements de l'informatique théorique.

Nous allons passer en revue dans cet article, en complément du précédent, quelques unes des différences entre information classique et information quantique. Précisons, avant cet examen, que nous adopterons une vue «physicienne» de l'information et que nous ne traitons évidemment pas d'information sémantique (le sens d'un mot, d'un texte, d'une musique, etc.) ou d'autres notions d'information destinées à cerner des contenus non symboliques.

Le lecteur quantique modifie le livre

Dans le monde classique, la consultation de l'information n'en modifie pas la teneur : lire un livre n'en change pas le texte, consulter un site Internet le laisse inchangé. Dans le monde classique, un objet est le même, qu'il soit connu ou pas. En revanche, l'ac-



1. INFORMATION ALÉATOIRE ET DUPLICATION INTERDITE. Un photon se propage selon une direction de polarisation perpendiculaire à son axe de propagation. Cette direction de polarisation est caractérisée par un angle *a*, 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 *a* égale 0, sera intercepté si *a* égale 90°, et passera avec une probabilité $\cos^2 a$ pour les angles intermédiaires. La détection ou non du photon est donc insuffisante pour connaître l'angle *a*. Dans une suite de photons ayant chacun un angle de polarisation égal à 45 degrés, la probabilité que chaque photon soit détecté après passage par le filtre est 1/2. En passant par le filtre polarisant, le photon perd son orientation primitive, ce qui rend l'angle *a* définitivement inconnaissable et le photon impossible à dupliquer.

quisition de l'information sur certains systèmes quantiques les perturbe irrémédiablement. C'est une conséquence du principe d'incertitude d'Heisenberg : mesurer une grandeur associée à un objet interdit d'en connaître d'autres ; plus grave, elle en fait un autre objet. L'information quantique a une réalité physique différente de l'abstraction de l'information classique.

Cette propriété quantique selon laquelle la mesure modifie l'objet mesuré trouble depuis longtemps ceux qui tentent de comprendre la mécanique quantique. Un exemple de cette difficulté, la détermination de la direction de polarisation d'un photon, est détaillée sur la figure 1.

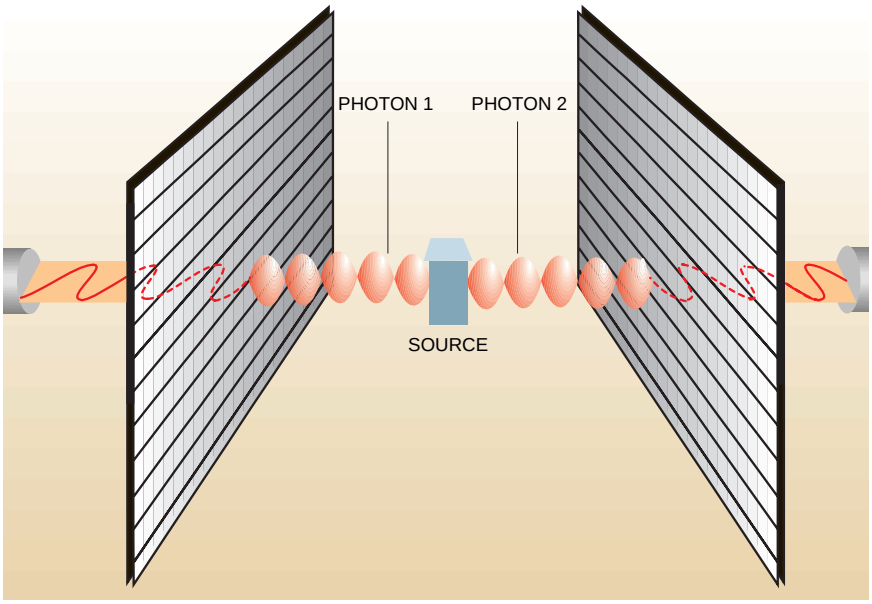
Informations aléatoires et indéterminisme

Cet exemple du photon montre aussi que l'information quantique est parfois authentiquement aléatoire : si, après avoir polarisé un photon selon une direction *a*, on le fait passer dans un filtre polarisant dont l'axe fait un angle de 45° avec *a*, on le détectera exactement une fois sur deux. En envoyant dans le dispositif une série de photons identiques, on obtient une suite de détections symbolisée par une suite de 1 et de 0 (1 pour une détection ; 0 pour une absence de détection) qui possède toutes les propriétés attendues d'une suite de 0 et de 1 parfaitement aléatoire. De telles suites sont intéressantes pour des méthodes de calcul comme la méthode de Monte-Carlo ou le cryptage des informations. Aussi cette propriété a-t-elle conduit à proposer des générateurs de bits aléatoires fondés sur des mécanismes quantiques *(voir la rubrique* Logique et calcul *du mois de mars 1998, qui traite des suites aléatoires en informatique)*.

Copier l'information

Les moines du Moyen Âge, nos photocopieuses et les lecteurs de disquette de nos ordinateurs copient des informations sans rencontrer d'obstacles fondamentaux. Dupliquer l'information classique et en faire de multiples versions est facile et ne coûte presque rien. Comme cette information n'est pas de nature physique, elle n'est pas liée à son support, et elle est donc copiable. Dans le monde quantique, la copie n'est pas toujours possible. Le principe de non-duplication («no-cloning principle») énoncé par W. Wootters, W. Zurek et D. Dieks en 1982 exprime cette impossibilité : un état quantique inconnu ne peut pas être dupliqué.

Reprenons l'exemple du photon : vous ne réussirez jamais à dupliquer un photon dont vous ne savez rien, car vous ne pourrez jamais connaître complètement son état quantique. Si vous essayez, dès que vous commencez à mesurer certaines quantités observables (la polarisation selon une direction par exemple), vous détruisez l'état quantique du photon et vous ne pouvez mesurer d'autres observables. Cette impossibilité interdit la duplication. Notons quand même que le principe de non-duplication n'empêche pas la création de plusieurs objets identiques (par exemple, plusieurs photons de même polarisation) lorsque l'information liée aux objets est connue, car elle résulte du moyen de fabrication.



2. PHOTONS CORRÉLÉS ET INFORMATION ÉTALÉE. On sait produire des paires de photons corrélés, c'est-à-dire dont les directions de polarisation sont inconnues, mais identiques. Une telle paire contient une information non locale, possibilité exclue dans le monde classique. Cette non-localité de l'information se manifeste de la manière suivante : si l'on dispose sur le trajet des photons des filtres polarisants de même orientation, les deux photons corrélés émis par une source seront tous les deux interceptés ou tous les deux transmis, quelle que soit la distance qui sépare les photons au moment de la mesure (on a mené des expériences où les photons sont séparés l'un de l'autre de 10 kilomètres). Tout se passe comme si le premier photon savait comment l'autre se comporte : aussi faut-il admettre que deux photons corrélés forment un objet physique unique qui contient une information étalée dans tout l'espace.

Cacher l'information, et distribuer des clefs secrètes

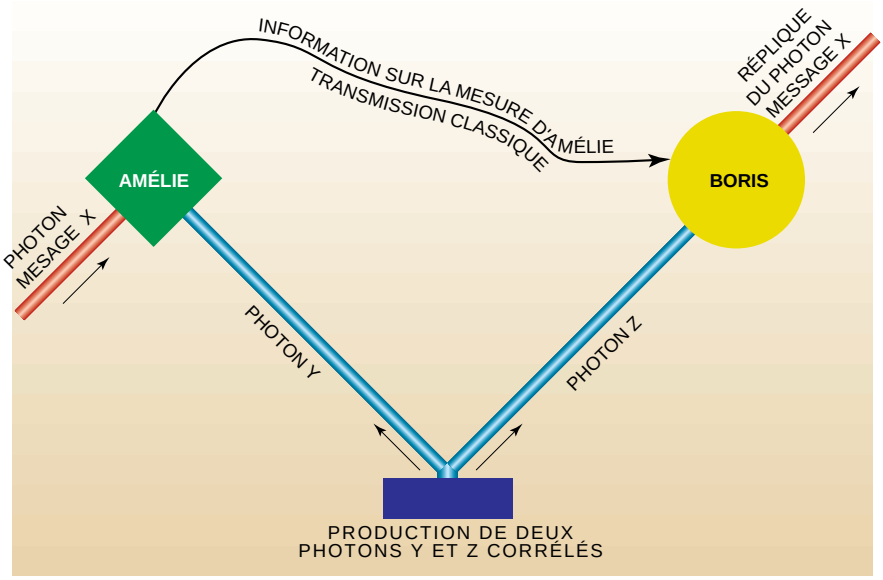
Cacher de l'information classique – ce qui est le but de la cryptographie – est théoriquement difficile : la plus grande partie des méthodes de cryptographie mathématique utilisées aujourd'hui se fonde sur des conjectures non démontrées et sont donc incertaines. Cet état de fait arrange les agences de renseignements, qui laissent croire que les codes légalement autorisés sont inviolables, alors qu'elles savent déchiffrer certains d'entre eux.

En revanche, la cryptographie quantique, qui utilise le principe de non-duplication des photons quantiques, propose des méthodes de distribution de clefs secrètes sûres et sans équivalent classique. Ces méthodes garantissent absolument le secret des échanges.

La cryptographie quantique est aujourd'hui suffisamment développée pour qu'avec des fibres optiques on sache distribuer des clefs secrètes entre des points distants de plusieurs dizaines de kilomètres. L'utilisation commerciale ou militaire de ces méthodes est sur le point de se faire (et a peut-être déjà eu lieu... de manière secrète).

Isoler l'information : la non-localité

Une autre propriété singulière de l'information quantique, étrange et difficile à comprendre, est la non-localité :



3. LA TÉLÉPORTATION QUANTIQUE est un moyen de faire voyager de l'information inconnue (un état quantique) à la vitesse de la lumière. Amélie veut transmettre l'état quantique d'un photon X à Boris. Elle ne peut prendre totalement connaissance de cet état quantique et doit quand même le communiquer par radio à Boris. Pour réaliser la téléportation de l'état quantique de X, Amélie et Boris créent une paire de photons corrélés Y et Z ; Amélie garde Y et Boris garde Z. (Les photons Y et Z pourront, peut être, un jour être créés et stockés avant qu'Amélie et Boris ne s'éloignent l'un de l'autre ; aujourd'hui, les photons corrélés sont créés entre Amélie et Boris et leur sont envoyés.) Amélie fait interagir X avec Y, ce qui lui fournit une information classique, qu'elle envoie par radio à Boris. Grâce à celle-ci, Boris peut opérer une transformation de Z qui place Z dans l'état quantique de X, lequel a donc été recréé. Dans une telle opération, en théorie applicable à des systèmes quantiques plus complexes, l'information quantique a été séparée en deux composantes, l'une classique qui voyage à la vitesse de la lumière par le signal radio, l'autre quantique qui voyage en quelque sorte instantanément par utilisation de la corrélation entre Y et Z. Le principe d'inconnaissabilité n'est pas violé, car ni Amélie ni Boris n'ont eu connaissance de l'état quantique téléporté X. Le principe de non-duplication est respecté lui aussi, car X, lors de la combinaison de X avec Y, a été détruit par Amélie.

une information quantique peut ne pas être localisée en un endroit précis, mais être diffuse dans l'espace entier comme si on l'avait parfaitement étalée . John Bell a en effet établi en 1964 que les prévisions de la mécanique quantique ne peuvent être reproduites par aucune théorie où chaque information est située en un point précis de l'espace.

Les conclusions de Bell ont été vérifiées par Alain Aspect, Jean Dalibard, Philippe Grangier et Gérard Roger en 1982 *(voir la figure 2)* : l'information n'est ni dans l'un des composants du système ni dans un autre, mais dans l'ensemble. J. Bell a ainsi montré que l'on pouvait coder l'information dans les corrélations entre diverses parties éloignées d'un système physique (possibilité qui est, par définition, exclue du modèle général des ordinateurs classiques où, à chaque instant, chaque information est localisée) et que l'on peut manipuler cette information non locale. Cette propriété confère une puissance supérieure au calcul quantique, et les expériences de calcul quantique de ces derniers mois ont confirmé les prévisions des modèles théoriques.

La transmission d'une information dans le monde classique (relativiste) peut se faire à la vitesse de la lumière : il suffit d'envoyer un signal lumineux ou radio qui contient l'information que l'on veut faire voyager.

On ne peut, en principe, pas transmettre l'information d'un état quantique par codage d'un signal lumineux, car cette information est inconnue ; on pourrait alors envisager de transmettre le système quantique lui-même, mais, s'il possède une masse, il est impossible de le faire à la vitesse de la lumière. L'information quantique voyagerait-elle moins bien que l'information classique?

La téléportation

Il n'en est rien : la technique de téléportation, proposée 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 *(voir la figure 3)*. Grâce à cette méthode étonnante (dont on se demande pourquoi elle n'a pas été découverte plus tôt), l'information quantique voyage aussi vite que l'information classique. En revanche, la non-localité de l'information quantique n'autorise pas la transmission de l'information à une vitesse supérieure à celle de la lumière : dans l'expérience avec les deux photons corrélés, je peux, en mesurant la polarisation de mon photon, certes connaître instantanément celle de mon partenaire éloigné, mais ce n'est pas un échange : celui-ci ne peut me transmettre instantanément une information choisie par lui.

Soulignons une particularité : la méthode de téléportation quantique, qui utilise des paires de photons corrélés (de l'information non locale), oblige que l'on détruise à son point de départ l'état quantique qu'on veut déplacer (si cela n'était pas le cas on pourrait le dupliquer, ce qui est interdit). De surcroît, ni l'émetteur ni le récepteur ne peuvent connaître complètement l'information qu'on fait ainsi voyager, car lire l'information, c'est la détruire.

Ainsi, dans le monde quantique, la situation est nette : on peut transférer à la vitesse de la lumière l'information décrivant un système quantique, mais à la condition incontournable que le système complexe soit détruit en son point de départ et qu'on n'en prenne pas connaissance. Les auteurs de science-fiction semblent avoir deviné cette règle : dans *Star Trek*, par exemple, la téléportation qu'utilise l'équipage du vaisseau *Entreprise* pour de petites distances s'accompagne – sauf accident – de l'annihilation au point de départ du voyageur.

Les méthodes quantiques de téléportation ne sont pas seulement de la science-fiction, et si l'on est très loin de téléporter un être humain une équipe autrichienne a réussi, il y a quelques mois, à appliquer la méthode à l'état quantique d'un photon *(voir La téléportation quantique*, in Pour La Science, *février 1998, page 30)*.

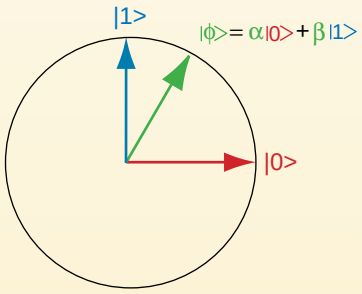
La téléportation quantique pourrait devenir utile, car elle est en mesure de régler le problème qui fait que la cryptographie quantique ne peut fonctionner que sur des distances limitées

PROPRIÉTÉS DE L'INFORMATION QUANTIQUE

a

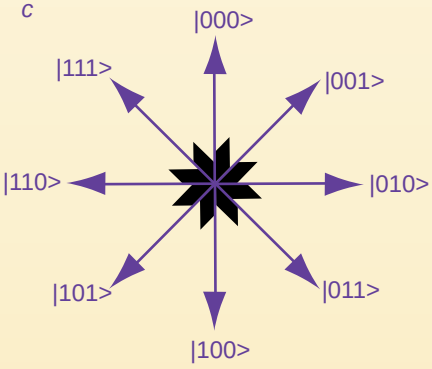
a) L'information unitaire classique est le bit : un objet qui vaut 0 ou 1.

b



b) 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 est nul sont orthogonaux). Les éléments d'une base orthogonale sont fixés et notés |0> et |1>. Un qubit $|\phi\rangle$ se représente sous la forme $\alpha\,|0\rangle + \beta\,|1\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$, où α et β sont des nombres complexes (ainsi le qubit est déterminé par quatre nombres réels)
Une mesure amène le qubit $|\phi\rangle$ sur l'un des vecteurs de la base |0>, |1>. 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 $|\beta|^2$

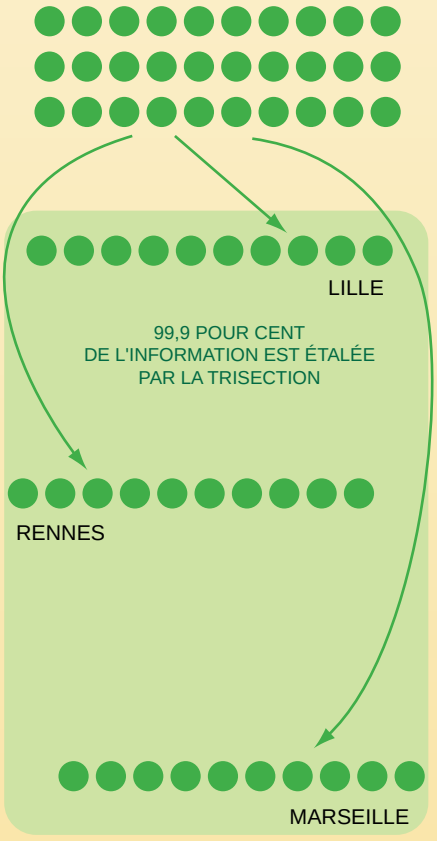
c



c) L'état quantique d'un N-qubit est un vecteur dans un espace analogue à celui du qubit, mais de dimension 2^N. On choisit une base orthogonale de cet espace.. 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 de la forme :
$a_{000}\,|000\rangle + a_{001}\,|001\rangle + a_{010}\,|010\rangle + a_{011}\,|011\rangle + a_{100}\,|100\rangle + a_{101}\,|101\rangle + a_{110}\,|110\rangle + a_{111}\,|111\rangle$,
où la somme des carrés des $|a_{ijk}|$ est égale à 1.
La lecture du 3-qubit donne un vecteur de la base, chaque vecteur de la base étant obtenu avec une probabilité proportionnelle à $|a_{ijk}|$.

d) 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). À 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>] / $\sqrt{8}$
Un N-qubit est un objet difficile à décrire : il faut, pour le spécifier complètement, indiquer 2^N nombres complexes.
Il n'était pas évident que les règles délicates du calcul quantique par transformations unitaires produisent des résultats intéressants. C'est pourtant ce qu'ont montré Peter Shor, Lov Grover et les algorithmiciens quantiques.

e



e) La non-localité : un résultat de Don Page
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 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, les composantes sont corrélées, et seules des mesures collectives peuvent la révéler.

CODE CORRECTEUR D'ERREUR DE PETER SHOR

Dans le code correcteur d'erreur classique le plus simple, on triple chaque information : on remplace 0 par (0, 0, 0) et 1 par (1, 1, 1). Quand on le juge nécessaire, on teste si les trois bits d'un tel triplet sont égaux et si ce n'est pas le cas on inverse le bit en exemplaire unique : si on lit (0,0,1) on rétablit (0,0,0), si on lit (1,0,1), on rétablit (1,1,1). Une telle méthode corrige toutes les erreurs simples. Si la probabilité d'une erreur simple est petite alors celle d'une erreur double ou triple (non-corrigée par la méthode) sera très petite et on la néglige.
L'adaptation par Peter Shor de ce code correcteur commence par remplacer chaque qubit |0> par le 3-qubit |000> et chaque qbit |1> par le 3-qubit |111>.
La méthode classique de correction est inapplicable car il faudrait lire chacune des composantes des 3-qubit, ce qui est impossible sans perturber fatalement les 3-qubits. En revanche une mesure collective non destructive de deux composantes est possible par la méthode de Shor.
Si on a le qubit |x,y,z> on peut par exemple connaître x XOR y. (x XOR y désigne le OU exclusif, aussi dénommé NON contrôlé, entre x et y qui vaut 0 si x et y sont égaux et 1 sinon). L'idée de Shor est de calculer la paire [y XOR z, x XOR z].
Un petit calcul montre que si une seule des composantes a basculé (0 devenu 1, ou 1 devenu 0) dans un 3-qubit composé de trois fois la même composante, alors la paire de Shor donne l'écriture en binaire du numéro du bit qui a changé. On peut alors effectuer la correction.
Exemple : Pour (0,1,0) y XOR z vaut 1, x XOR z vaut 0, donc la paire de Shor est [1,0], qui donne 10, l'écriture binaire de 2, le numéro de la composante à corriger.
Le secret de la méthode de correction (sans contradiction avec le principe de non-duplication) réside dans le fait (a) qu'on ne lit aucune composante individuellement, (b) qu'on trouve le numéro de la composante à corriger, et (c) qu'on la corrige sans même savoir si on change un 0 en 1 ou l'inverse.

(moins de 100 kilomètres). En cryptographie quantique, on utilise des photons qu'on fait circuler dans des fibres optiques, où ils sont inévitablement atténués par absorption. L'idée d'utiliser des répéteurs classiques qui lisent le signal et l'amplifient est inapplicable, car les photons qui circulent sont dans des états quantiques inconnus et, encore une fois, pour les amplifier, il faudrait les lire. La technique de téléportation résout en principe le problème et autorise la conception de nouveaux répéteurs qui «ré-émettent» sans lire les photons envoyés.

Mémoriser l'information : la superposition et le qubit

Après ces considérations générales sur les propriétés de la transmission quantique, examinons le support de cette information. Le support élémentaire classique est le bit : un 0 ou un 1 ; son analogue quantique est le qubit, le *quantum bit*. Classiquement ou quantiquement, le bit est l'état de n'importe quel système matériel pouvant prendre un parmi deux états différents, par exemple un curseur tourné vers le haut ou vers le bas, un carré noir ou blanc sur un papier, un accumulateur électrique chargé ou non, le spin d'un noyau d'atome orienté vers le haut ou vers le bas, etc. Quelle est alors la différence entre un bit et un qubit?

Les principes de la mécanique quantique autorisent qu'un chat soit à la fois mort et vivant – ce que l'on appelle la superposition d'états. Aussi le qubit décrit, avec deux nombres a et b, un état $a\ |0\rangle + b\ |1\rangle$ (a et b sont des nombres complexes). Il mémorise ainsi plus d'informations qu'un bit classique. Le N-bit, de la forme 00101011... est décrit complètement par n choix de chiffres 0 ou 1, le N-qubit est spécifié par 2^N choix de nombres complexes *(voir Les propriétés de l'information quantique, page précédente)*.

Ainsi, avec un 2-qubit, on mémorise simultanément 4 nombres complexes a, b, c, d, avec un 10-qubit, on mémorise un millier de nombres, avec un 30-qubit, on atteint le milliard, et avec un 40-qubit, on pourrait en principe stocker tout le contenu disponible actuellement sur le réseau Internet (qu'on évalue à 8 000 milliards de caractères, ce qui équivaut à une bibliothèque de 8 millions de livres).

Calculer avec des qubits revient finalement à faire simultanément plusieurs calculs à la fois : avec un 3-qubit par exemple 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), car calculer avec des états superposés, c'est faire des calculs simultanés. Bien sûr, la maîtrise de ces superpositions ne va pas de soi, mais on comprend l'intérêt d'y parvenir.

Il y a trois ans, certains théoriciens de la mécanique quantique pensaient que les phénomènes d'instabilité rendraient à jamais impossibles les calculs quantiques qui nécessitent la création de N-qubits, leur préservation durant des intervalles de temps significatifs, leur manipulation et leur lecture.

L'obstacle fondamental invoqué était la décohérence, c'est-à-dire la propension qu'un état quantique complexe (un N-qubit, par exemple) a d'interagir spontanément avec l'environnement, ce qui, en projetant son état sur l'un des états de base, détruit une partie de son contenu en information. Cette interaction agit comme une lecture conduisant à un état non superposé, par exemple celui codant (0,0,0), ce qui évidemment fait perdre tout son intérêt au N-qubit.

Tout a changé en 1996 et 1997, quand on a compris qu'on pouvait limiter toutes ces sources d'instabilité par des techniques de correction d'erreurs.

Les codes correcteurs d'erreurs

La théorie classique de la correction d'erreur conduit, même avec des composants imparfaits, à mener des calculs justes. Son adaptation au cas quantique est une avancée remarquable *(voir l'encadré Code correcteur d'erreur de Peter Shor)*, qui offre la perspective d'une préservation parfaite d'états quantiques complexes, préservation jugée impossible à cause de processus irréversibles comme la relaxation par émission spontanée.

Dans un calcul utilisant des méthodes de correction, chaque élément d'un qubit pourrait être perdu et reconstitué. Peter Shor (inventeur de l'algorithme de factorisation quantique mentionné plus loin) et Andrew Steane remarquèrent, en 1995, que les méthodes classiques de correction d'erreurs s'adaptaient. Cela paraissait à première vue difficile, car le principe de non-duplication empêche la copie redondante d'une même information à préserver, copie qui est à la base de la correction d'erreur clas-

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?

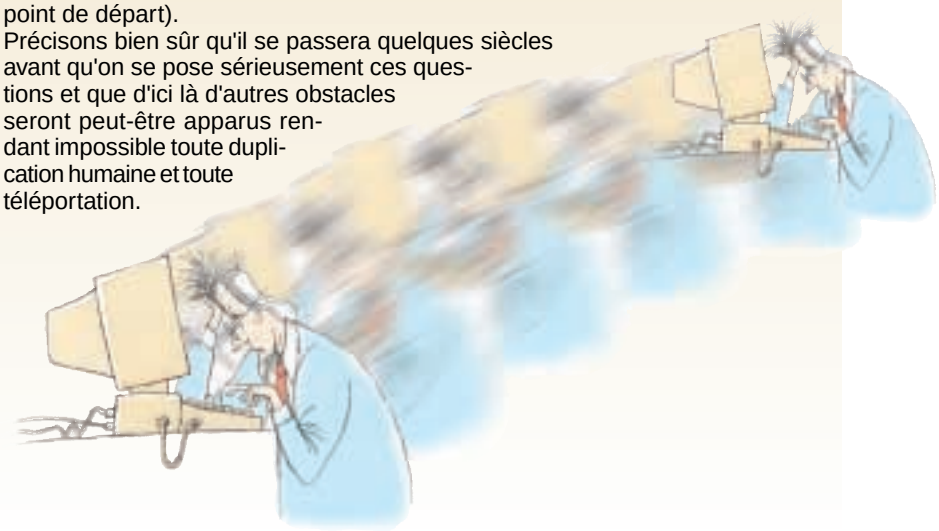
Si l'on pense qu'une personne humaine n'est pas seulement définie par l'état physique de son corps et de son cerveau (question philosophique) alors aucune discussion n'est possible. Supposons donc que l'intégrité d'une personne humaine n'est qu'une question physique. Deux cas apparaissent.

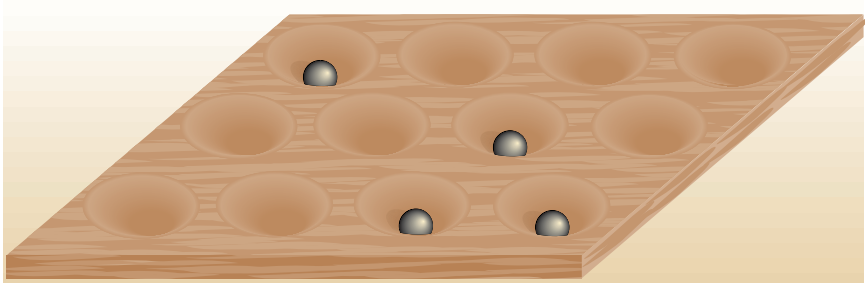
Cas 1. La mécanique quantique ne joue pas de rôle essentiel dans le fonctionnement du corps et du cerveau. En prenant connaissance à un niveau de détail assez fin de la position des atomes qui composent le voyageur (chose peut-être impossible mais qu'aujourd'hui aucun principe n'interdit) on pourrait 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.