Des quanta et des bits: les mystères de l'information quantique

Nicolas Cerf[1] et Nicolas Gisin[2]

Nous avons tous entendu parler de la révolution de notre société de l'information par les réseaux informatiques comme Internet ou les nouvelles technologies de communication par fibre optique ou par satellite. Mais l'on sait moins que la notion d'information est aussi l'objet d'une théorie mathématique, établie par Claude Shannon peu après la deuxième guerre mondiale, qui est l'un des piliers des télécommunications modernes. Depuis le codage de la musique sur un disque compact jusqu'à la réception des images lointaines des satellites de Jupiter par la sonde spatiale Galileo, toutes ces réalisations reposent en grande partie sur la théorie de l'information de Shannon. Malgré le spectre d'applications remarquablement vaste de cette théorie, Claude Shannon ne soupçonnait sans doute pas que des chercheurs allaient découvrir, quelques décennies plus tard, un prolongement surprenant de ses travaux dans le monde quantique tel qu'il se manifeste à l'échelle atomique. Lorsque le support des données stockées ou transmises est un atome isolé ou un simple photon, les manifestations de la mécanique quantique bouleversent le concept même d'information et donnent lieu à des phénomènes étranges comme la possibilité de téléporter un bit quantique ou la "non-copiabilité" d'un quantum d'information (qui est à la base de la cryptographie quantique). Parallèlement, les scientifiques ont pu démontrer que certaines notions standard de la théorie de Shannon comme la compression de données ou la correction des erreurs qui surviennent dans une ligne de transmission peuvent être adaptées à l'échelle atomique. De tels exemples montrent à quel point la mécanique quantique déjoue notre intuition classique et nous réserve encore bien des surprises.

Tout procédé de transfert d'information d'un point à l'autre, que ce soit la propagation d'ondes sonores associée à la conversation entre deux personnes, les signaux électriques transitant dans un fil téléphonique, ou encore les ondes lumineuses parcourant la distance entre un objet et nos yeux, peut être décrit de manière générale comme un canal de communication. Un tel canal est pratiquement toujours sujet à des perturbations ou à du bruit, en conséquence de quoi le signal reçu n'est pas parfaitement fidèle au signal émis. Par exemple, les parasites dans une mauvaise ligne téléphonique peuvent rendre la voix d'un interlocuteur infidèle voire inintelligible. Jusqu'à l'après-guerre, on pensait que la seule façon d'augmenter la fiabilité d'une communication était d'améliorer le canal ou d'augmenter la puissance du signal pour vaincre le bruit. Il faut par exemple élever la voix dans une salle bruyante pour se faire comprendre. En 1948, le jeune mathématicien Claude Shannon créa la surprise en montrant au contraire que tout canal, aussi bruyant soit-il, peut être utilisé pour communiquer avec une qualité arbitrairement bonne à condition d'introduire de la redondance dans le signal.[3] La théorie sous-jacente est basée sur le codage de l'information et l'usage de codes correcteurs d'erreur. Une application de ces idées dans notre vie quotidienne est l'enregistrement musical sur un disque compact: même si le disque est rayé—jusqu'à un certain point—la reproduction du son est intacte.

Au cours de la dernière décennie, il s'est avéré que ce domaine des sciences de l'information, jusque là essentiellement du ressort des ingénieurs, avait un prolongement inattendu dans le monde quantique. Un premier pas dans cette aventure remonte au début des années 60, lorsque

[1]Nicolas Cerf est Chargé de Cours à l'Ecole Polytechnique de l'Université Libre de Bruxelles et *Senior Research Fellow* au *California Institute of Technology* de Pasadena aux Etats-Unis. Adresse électronique: `Nicolas.Cerf@ulb.ac.be`

[2]Nicolas Gisin est Professeur à l'Université de Genève où il dirige la section d'optique du Groupe de Physique Appliquée. Adresse électronique: `Nicolas.Gisin@physics.unige.ch`

[3]C. Shannon, *Bell System Technical Journal*, 27, 379-423 et 623-656, 1948.

le physicien américain Rolf Landauer du laboratoire de recherche de IBM à Yorktown Heights défendit l'idée que l'information[4] n'est pas un concept mathématique abstrait, détaché de toute réalité matérielle, mais est en fait de nature physique. Une information est toujours portée par un support physique, que ce soit les molécules d'encre sur une page de journal, la magnétisation des atomes constituant un disque d'ordinateur, ou encore le flot d'électrons parcourant un fil téléphonique. En deux mots, il n'y pas d'information sans représentation physique, et tout procédé de traitement de l'information est en définitive accompli par un processus physique. La contribution de Rolf Landauer fut surtout de comprendre la portée de ce caractère "matériel" de l'information. En particulier, il montra que le stockage d'un bit d'information (un 0 ou un 1) nécessite toujours au minimum la dissipation irréversible d'un quantum d'énergie égal à $kT\ln(2)$, où T est la température du support au sein duquel l'information est enregistrée et k est la constante de Boltzmann. Le traitement de l'information (stockage, calcul, transmission, etc.) est en ce sens indissociable de la thermodynamique du système physique au sein duquel il se déroule.

La nature physique de l'information implique la manifestation d'effets quantiques lors de la manipulation de bits à l'échelle atomique.

Le constat de la nature physique de l'information, qui peut apparaître presque comme une tautologie lorsque l'information est portée par un support macroscopique, prend une dimension nouvelle si les bits d'information sont stockés ou transmis par des éléments de taille atomique. L'information à laquelle nous sommes accoutumés, caractérisée par une séquence de 0 et de 1 (des bits), a en effet une représentation intrinsèquement classique car elle met en jeu un nombre important de particules. Un exemple parlant est le stockage d'un bit par la charge d'une capacité au sein de la mémoire vive dynamique d'un ordinateur: un bit correspond à la présence (ou l'absence) de l'ordre d'un milliard d'électrons dans chaque cellule de mémoire pour les technologies actuelles, de sorte qu'une description classique de l'information est largement suffisante. L'information classique est donc celle avec laquelle nous sommes familiers, qui peut être copiée et traitée sans limite. Cette page de La Recherche constitue un exemple d'information classique. On peut la photocopier et créer un double de qualité en principe parfaite si l'on fait abstraction des limitations technologiques. On peut aussi la numériser et la convertir en données traitées dans un ordinateur, un exemple typique de système manipulant de l'information classique. Par contre, lorsqu'une particule individuelle (par exemple un atome ou un photon) est le support d'un bit, l'information correspondante doit nécessairement être traitée dans le cadre de la mécanique quantique, seule théorie connue capable de prédire le comportement de la matière à l'échelle atomique. L'état de polarisation d'un photon peut par exemple représenter ce que l'on appelle un "bit quantique" (un q-bit). On peut conventionnellement identifier la polarisation horizontale du photon à l'état quantique $|0\rangle$, et la polarisation verticale à l'état $|1\rangle$. Si l'on mesure le q-bit en disposant un filtre de polarisation verticale sur la trajectoire du photon, la détection du photon sera associée à un 1, alors que sa non-détection équivaudra à un 0. Plus généralement, un q-bit est représenté par un vecteur dans un espace de Hilbert[5] de dimension 2, dont les éléments de base sont notés $|0\rangle$ et $|1\rangle$. Comme on va le voir, la mécanique quantique donne lieu à un nombre de propriétés singulières et totalement insoupçonnées du concept sous-jacent d'information à l'échelle atomique.

[4] Nous nous limitons dans cet article au cas de l'information numérique (ou digitale), c'est-à-dire constituée d'une séquence de chiffres binaires, des 0 et des 1 (des bits), et nous ne considérons pas les signaux continus.

[5] Un espace de Hilbert est un espace vectoriel complexe munis d'un produit scalaire. Les éléments d'un tel espace de dimension 2 sont des vecteurs à deux composantes complexes $\binom{a}{b}$ que l'on peut aussi noter $a|0\rangle + b|1\rangle$. Le conjugué hermitien de $\binom{a}{b}$ est défini comme $(a^* \ b^*) = a^*\langle 0| + b^*\langle 1|$, où l'opération $*$ est la conjugaison complexe. On peut écrire le produit scalaire entre deux vecteurs $\binom{a}{b}$ et $\binom{\alpha}{\beta}$ comme $(a^* \ b^*)\binom{\alpha}{\beta} = a^*\alpha + b^*\beta$.

Les superpositions quantiques bouleversent notre intuition de la notion d'information dans le monde microscopique.

L'une des particularités remarquables de la mécanique quantique est de prédire l'existence de superpositions quantiques.[6] Un photon peut se trouver dans un état qui est une superposion des deux états de polarisation, horizontale et verticale. En d'autres termes, le q-bit correspondant est alors décrit par une superposition de $|0\rangle$ et de $|1\rangle$, par exemple l'état $\alpha|0\rangle + \beta|1\rangle$ où les amplitudes complexes α et β satisfont la condition de normalisation $|\alpha|^2 + |\beta|^2 = 1$. Un q-bit dans un tel état n'a pas d'analogue classique: un bit classique peut être 0 ou 1, mais jamais dans un état intermédiaire! Si l'on mesure un q-bit dans cet état, on obtient le résultat 0 avec la probabilité $|\alpha|^2$ ou 1 avec la probabilité $|\beta|^2$. Cependant, il est erroné d'en conclure que le q-bit est une sorte de bit aléatoire, comme si l'on tirait au hasard une boule d'une boîte contenant des boules noire et des boules blanches et que l'on associait la couleur de la boule sélectionnée à la valeur du bit. Seule la mesure du q-bit induit ces probabilités, et une mesure différente correspondant à la base formée par le vecteur $\alpha|0\rangle + \beta|1\rangle$ et le vecteur orthogonal $\beta^*|0\rangle - \alpha^*|1\rangle$ donnerait au contraire toujours le même résultat.

Prenons l'exemple d'un q-bit caractérisé par un photon dans une superposition uniforme des états de polarisation verticale et horizontale, c'est-à-dire dans l'état $(|0\rangle + |1\rangle)/\sqrt{2}$. Si un filtre polarisant vertical est placé sur la trajectoire du photon, ce dernier sera détecté une fois sur deux après le filtre. La détection du photon équivaut à la valeur 1 du bit, alors que l'absence de détection correspond à un 0. On pourrait en déduire que tout se passe comme si le photon avait été tiré au hasard d'un réservoir contenant une multitude de photons de polarisation pour moitié verticale, pour moitié horizontale. Cependant, si l'on place un filtre polarisant diagonal (dont l'orientation fait un angle de 45° avec l'horizontale), on constate que la présence du photon est toujours détectée. Le photon est donc en fait dans un état de polarisation diagonale, ce qui démontre que les probabilités de détection ou non-détection du photon lorsque l'on avait placé un filtre de polarisation verticale étaient induites par la mesure elle-même. A l'inverse, un photon polarisé verticalement (état $|1\rangle$ du q-bit) sera détecté avec une probabilité de 1/2 derrière un filtre polarisant diagonal car il correspond à une superposition uniforme d'un photon de polarisation diagonale $(|0\rangle + |1\rangle)/\sqrt{2}$ et anti-diagonale $(|0\rangle - |1\rangle)/\sqrt{2}$. La théorie quantique de l'information a pour objet de comprendre et d'exploiter les curiosités qui résultent de ce principe de superposition en terme d'information.

Il n'existe pas de "photocopieuse" quantique qui permette de copier un bit quantique sans le perturber.

Une première surprise est la découverte en 1982 par les physiciens William Wootters de Williams College, Wojciech Zurek du laboratoire américain de Los Alamos, et Dennis Dieks de l'Université d'Utrecht qu'il est fondamentalement impossible de dupliquer l'information quantique.[7] Plus précisément, un état quantique inconnu (ou une superposition arbitraire d'états quantiques) ne peut être dupliqué parfaitement. Revenons à l'exemple d'un photon dont l'état de polarisation représente un bit quantique. Si l'on se limite à un photon ayant obligatoirement l'une des deux polarisations, horizontale ou verticale, il est facile de détecter sa présence derrière un filtre polarisant vertical, et d'émettre ensuite deux photons de polarisation verticale s'il y a détection, ou deux photons de polarisation horizontale dans le cas contraire. Pourtant, une telle procédure ne permet pas la violation du principe de non-duplication car

[6]Le principe de superposition et en particulier le "chat de Schrödinger", l'une de ses manifestations les plus étonnantes, est discuté en détail dans "*Le chat de Schrödinger se prête à l'expérience*", La Recherche n° 301, Septembre 1997.

[7]W. K. Wootters et W. H. Zurek, *Nature*, 299, 802, 1982; D. Dieks, *Phys. Lett.*, 92A, 271, 1982.

le q-bit correspondant n'est pas dans un état arbitraire et admet une description sous-jacente classique (on peut le voir comme un bit classique). Considérons en effet un photon de polarisation diagonale, et tentons de le dupliquer à l'aide du dispositif précédent. On obtient soit deux photons de polarisation horizontale, soit deux photons de polarisation verticale, alors que le résultat attendu est deux photons de polarisation diagonale. Il est facile de se convaincre que la duplication est effectivement imparfaite en disposant un filtre polarisant diagonal sur le trajet des deux photons issus de ce processus. Chacun de ces photons est détecté avec une probabilité de $1/2$, alors que l'on devrait les détecter dans tous les cas s'ils étaient des copies conformes du photon original. Cet exemple souligne l'impossibilité de construire un dispositif capable de dupliquer parfaitement à la fois les états de polarisation horizontale ou verticale (les états $|0\rangle$ et $|1\rangle$), et les états de polarisation diagonale (les états $(|0\rangle \pm |1\rangle)/\sqrt{2}$).

Bien sûr, la machine copieuse ne doit pas nécessairement impliquer une mesure (la détection du photon dans le processus ci-dessus). On peut concevoir une machine copieuse abstraite qui reproduirait parfaitement les états $|0\rangle$ et $|1\rangle$, produisant respectivement l'état $|00\rangle$ ou l'état $|11\rangle$. Cependant, si l'on tente de copier l'état de polarisation diagonale $(|0\rangle + |1\rangle)/\sqrt{2}$ avec cette machine, la propriété de linéarité de la mécanique quantique implique que l'état résultant sera $(|00\rangle + |11\rangle)/\sqrt{2}$ alors qu'une duplication parfaite devrait donner l'état produit $(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)/2$. Ce dernier état peut être réécrit comme $(|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$, et est donc bien distinct de l'état effectivement produit par cette copieuse puisqu'il contient les composantes $|01\rangle$ et $|10\rangle$, ce qui souligne l'incompatibilité entre l'exigeance d'une copie parfaite des états $|0\rangle$ et $|1\rangle$, et simultanément des états $(|0\rangle \pm |1\rangle)/\sqrt{2}$. En fait, si l'on souhaite que tous les états soient copiés de façon identique, on doit alors admettre une copie de qualité imparfaite (voir encadré sur la copieuse quantique universelle).

Copieuse quantique universelle:
En 1996, le physicien slovaque Vladimir Buzek a découvert, en collaboration avec le physicien américain Mark Hillery, qu'il est en théorie possible de définir une machine copieuse "universelle", qui copie aussi bien (mais pas parfaitement!) tout état d'un q-bit.[a] Cette copieuse est définie par la transformation unitaire qu'elle effectue sur le q-bit original ainsi que deux q-bits auxiliaires utilisés l'un pour y placer la copie et l'autre par la machine copieuse elle-même. La copieuse universelle transforme les états $|0\rangle$ et $|1\rangle$ comme suit:

$$\begin{aligned}|0\rangle &\rightarrow \sqrt{\frac{2}{3}}|00\rangle|0\rangle + \sqrt{\frac{1}{6}}(|01\rangle + |10\rangle)|1\rangle \\ |1\rangle &\rightarrow \sqrt{\frac{2}{3}}|11\rangle|1\rangle + \sqrt{\frac{1}{6}}(|01\rangle + |10\rangle)|0\rangle\end{aligned}$$

où les trois q-bits correspondent (de gauche à droite) à l'original, la copie, et un q-bit utilisé par la copieuse. On peut montrer que cette copieuse agit de façon similaire sur l'état diagonal $|a\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Si l'on note $|b\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ l'état anti-diagonal orthogonal à $|a\rangle$, la copie de $|a\rangle$ obtenue en faisant la somme des résultats de la copie de $|0\rangle$ et de $|1\rangle$ (en vertu de la linéarité de la mécanique quantique) peut être réécrite comme

$$|a\rangle \rightarrow \sqrt{\frac{2}{3}}|aa\rangle|a\rangle + \sqrt{\frac{1}{6}}(|ab\rangle + |ba\rangle)|b\rangle$$

ce qui illustre l'universalité de cette copieuse: toute superposition arbitraire est copiée de la même manière.
Si l'on duplique un $|0\rangle$ ou un $|1\rangle$ à l'aide de cette copieuse universelle, on obtient pour chaque exemplaire (l'original perturbé et la copie imparfaite) un mélange statistique de l'état original ($|0\rangle$ ou $|1\rangle$) avec une probabilité 2/3 et d'un q-bit aléatoire (c'est-à-dire un mélange équiprobable de $|0\rangle$ et de $|1\rangle$) avec la probabilité 1/3. Il est facile de voir que la copie de l'état diagonal $|a\rangle$ donne un mélange de $|a\rangle$ et d'un q-bit aléatoire (mélange équiprobable des états $|a\rangle$ et $|b\rangle$) dans les mêmes proportions. En fait, quelle que soit la superposition que l'on souhaite dupliquer, les deux exemplaires issus de la machine ne sont fidèles à l'original qu'avec une probabilité égale à 2/3 (ils sont remplacés par un q-bit aléatoire avec une probabilité 1/3). En quelque sorte, une copie parfaite n'est permise au mieux qu'avec une probabilité de 2/3, et d'ailleurs on peut montrer qu'une probabilité supérieure à cette valeur rendrait possible une communication instantanée en désaccord avec le principe de relativité restreinte.[b]

[a] V. Buzek et M. Hillery, *Phys. Rev.*, A 54, 1844, 1996.
[b] N. Gisin, *Phys. Lett.*, A 242, 1, 1998.

Le principe de non-duplication quantique permet la protection d'information secrète que l'on ne peut découvrir sans la perturber.

Au lieu d'être vu comme une loi limitative, intrinsèque à notre monde quantique, le principe de non-duplication quantique peut être tourné à notre avantage lorsque le but est au contraire de garder de l'information secrète. L'interdiction de copier parfaitement (et sans le perturber) un état quantique suggère en effet qu'il est possible d'exploiter la mécanique quantique pour conserver de l'information à l'abris de toute écoute pirate. C'est ainsi que, suivant les travaux pionniers du physicien Stephen Wiesner du Massachusetts Institute of Technology dans les années 70, le concept de cryptographie quantique est né en 1984 à l'issue des travaux de Charles Bennett du laboratoire de recherche IBM à Yorktown Heights et de Gilles Brassard de l'Université de Monréal. Ils ont proposé une méthode de distribution de clefs secrètes qui utilise des photons (q-bits) pour transmettre les bits de clef. Les méthodes cryptographiques à clef secrète garantissent l'inviolabilité d'une communication si l'émetteur et le récepteur autorisé (et lui seulement!) détiennent une même chaîne secrète de bits aléatoires appelée clef. En conséquence de la théorie de Shannon, cette clef doit avoir au moins la longueur du message à transmettre pour que la communication soit totalement sûre. Supposons que l'émetteur (appelons le Alice) veuille partager une clef secrète avec le récepteur (Bernard) en vue de lui transmettre un message crypté. Le protocole quantique proposé par Bennett et Brassard est le suivant.[8] Pour transmettre un bit de clef, Alice choisit une fois sur deux d'utiliser soit la base des états de polarisation horizontale ou verticale, soit la base des états de polarisation diagonale. Dans le premier cas, Alice code le 0 et le 1 par les états $|0\rangle$ et $|1\rangle$, alors qu'elle utilise respectivement les états $(|0\rangle + |1\rangle)/\sqrt{2}$ et $(|0\rangle - |1\rangle)/\sqrt{2}$ dans le deuxième cas. Ce choix de base s'effectue au hasard, de sorte qu'Eric, un indiscret désireux d'intercepter la communication sans être repéré, ne peut prédire correctement la base utilisée qu'une fois sur deux. Comme on l'a vu plus haut, s'il pouvait prédire quand la base $\{|0\rangle, |1\rangle\}$ est utilisée, il pourrait faire l'usage d'une machine copieuse reproduisant parfaitement ces états de manière à laisser l'original intact tout en gardant une copie à analyser ultérieurement. De même, il pourrait employer une machine qui reproduit exactement les états $(|0\rangle \pm |1\rangle)/\sqrt{2}$ lorsque la base diagonale est utilisée. Cependant, s'il se trompe dans sa prédiction de la base du q-bit, ce qui se passe une fois sur deux en moyenne, il perturbe nécessairement l'original. On peut montrer en effet que toute fuite d'information vers Eric s'accompagne nécessairement d'une perturbation du q-bit transmis, perturbation qui est en principe détectable par Alice et Bernard. Lorsque Bernard a reçu le q-bit, Alice peut déclarer publiquement son choix de base puisqu'il est trop tard pour qu'Eric puisse exploiter cette information. Bernard mesure alors le q-bit dans la bonne base, et obtient donc un bit de clef intact dans le cas où Eric n'a pas intercepté le q-bit. Si Eric a tenté d'effectuer une copie du q-bit, celle-ci induit nécessairement une probabilité finie d'erreur du bit reçu par Bernard. Pour rendre la distribution de clef secrète inviolable, Alice et Bernard comparent alors une petite fraction de la clef, qui doit être révélée et donc perdue, ce qui permet d'assurer que le risque d'une écoute non-détectée est en-dessous d'un seuil admissible. En pratique, des protocoles plus compliqués sont utilisés pour "amplifier" le caractère secret de la clef, mais toujours au prix d'une réduction de la longueur de clef utilisable. Presque 15 ans après cette proposition initiale, la technique de cryptographie quantique est passée maintenant au stade de la démonstration expérimentale, et l'on parvient par exemple à distribuer des clefs secrètes par fibres optiques sur des distances de l'ordre de quelques dizaines de kilomètres (voir encadré sur la cryptographie quantique démontrée).

[8] C. H. Bennett et G. Brassard, *Proc. IEEE Conf. on Computers, Syst. and Signal Process.*, pp. 175-9, 1984.

La cryptographie quantique démontrée expérimentalement: Pour réaliser une expérience de cryptographie quantique, il faut tout d'abord maîtriser la production de photons individuels, puis contrôler la polarisation ou la phase de ces photons depuis la source jusqu'au détecteur, et finalement être capable de détecter des photons uniques. Nous ne mentionnerons ici que quelques solutions démontrées sur des dizaines de kilomètres utilisant des fibres optiques installées sur le terrain, à l'extérieur des laboratoires. Pour la source, toutes les expériences ont utilisé des impulsions lasers extrêmement ténues, de sorte que la probabilité d'avoir deux photons dans une impulsion non vide n'est que de quelques pour cents. Cette solution a l'avantage d'être simple à réaliser, mais des sources à flux contrôlé de photons sont attendues avec impatience! Pour la détection, une solution identique a également été retenue par tous les expérimentateurs: l'utilisation de photodiodes à avalanche en mode Geiger. Ces composants standards des télécommunications optiques modernes sont en amélioration constante. Afin de limiter le bruit, les premières expériences nécessitaient de refroidir les photodiodes à l'azote liquide, mais un refroidissement thermoélectrique est aujourd'hui suffisant. Finalement, les différentes démonstrations expérimentales se distinguent surtout par la manière d'encoder les q-bits et de les contrôler durant leur propagation. En 1993 le DERA anglais (Defense Research Agency) et l'entreprise privée BT (anciennement British Telecom) ont démontré la possibilité d'encoder les q-bits dans la phase des photons[a]. Pour cela Alice et Bernard disposent chacun d'un interféromètre avec un bras long et un bras court. Si les deux interféromètres sont rigoureusement identiques, une interférence constructive conduit le photon vers une sortie de l'interféromètre de Bernard. Par contre si un interféromètre diffère de l'autre d'une longueur correspondant à une demi longueur d'onde, alors le photon émergera de l'autre sortie de l'interféromètre de Bernard. Finalement, si les interféromètres diffèrent d'un quart de longueur d'onde, les deux sorties sont statistiquement équiprobables. Ainsi Alice code son q-bit en appliquant une phase sur son interféromètre soit de 0 soit d'une demi longueur d'onde (équivalent à la base verticale-horizontale dans le protocole en polarisation discuté dans le texte), soit $\pm$ un quart de longueur d'onde (correspondant aux polarisations diagonales). Ce même schéma a par la suite été testé par le groupe de Richard Hughes à Los Alamos. En 1995, l'un des auteurs et son équipe a utilisé un câble optique de Swisscom sous le lac de Genève pour démontrer la faisabilité de la cryptographie quantique en utilisant la polarisation comme porteur de q-bit.[b] Une difficulté commune à ces trois démonstrations est la nécessité de réaligner le système toutes les quelques secondes ou minutes, en fonction des vibrations et fluctuations thermiques. En effet, le moindre changement thermique ou mécanique affecte la polarisation et la phase des photons se propageant dans la fibre. Si ce changement est connu, Bernard peut en tenir compte, mais en cas de fluctuations continue, Alice et Bernard doivent continûment déterminer ce changement. L'un d'entre nous a toutefois développé, l'année dernière, une technique qui contourne ce problème grâce à un nouveau type d'interféromètre (impossible à expliquer sans schémas: schémas à disposition si jugé approprié)[c]. Tous ces travaux, et d'autres en cours dans le monde entier, pourraient conduire la cryptographie quantique à devenir la première application industrielle de la mécanique quantique au niveau des quanta individuels! L'Europe a décidé de coordonner ses efforts grâce à un projet ESPRIT dénommé EQSPOT, incluant des partenaires d'Angleterre, d'Autriche, d'Italie et de Suisse.

[a] P. D. Townsend et al., *Electron. Lett.*, 29, 634, 1993.

[b] A. Muller et al., *Nature*, 378, p. 449, 30 novembre 1995.

[c] A. Muller et al., *Applied Physics Lett.*, 70, 793, 1997; G. Ribordy et al., *Electron. Lett.*, 34, 2116, 1998.

Les codes quantiques correcteurs d'erreur sont un moyen de lutte efficace contre la décohérence.

Le principe de non-duplication quantique a amené les physiciens a conclure, un peu trop hâtivement comme on va le voir, que la préservation d'un état quantique arbitraire était une tâche impossible. En effet, si la duplication quantique était permise, on pourrait imaginer de préserver un état quantique contre les perturbations dues à l'environnement en le recopiant plusieurs fois, en s'inspirant des techniques à la base des codes correcteurs d'erreur. La théorie classique de la correction d'erreur montre en effet qu'il est possible de protéger des données contre le bruit en les recopiant plusieurs fois, par exemple, ou plus généralement en introduisant de la redondance. Le code classique le plus simple, dit "code à répétition", consiste à remplacer chaque bit par trois copies identiques: on substitue le 0 par 000 et le 1 par 111. Si l'un des trois bits est erroné après transmission, le bit émis peut être retrouvé un utilisant simplement la règle de la majorité. Si par exemple le premier bit est inversé, le 0 devient 100 alors que le 1 devient 011. Dans le premier cas, la majorité des trois bits est 0 et donc on rétablit le 0, alors que la majorité est 1 dans le deuxième cas, et l'on rétablit le 1. En d'autres termes, si le nombre de bits 1 reçus est égal à 0 ou 1, le bit original est 0, alors que si ce nombre est égal à 2 ou 3, le bit original est 1. Ce code est parfait à condition qu'il n'y ait pas plus d'une seule erreur par bloc de trois bits dans un long message, et au prix d'une réduction du taux de transmission par un facteur 3.

Vu l'apparente nécessité fondamentale de copier l'information pour la préserver, il paraît donc impensable d'appliquer des idées similaires pour protéger l'information quantique en vertu du principe de non-duplication. Cette hypothèse était admise par tous jusqu'à la fin de l'année 1995, lorsque l'américain Peter Shor des laboratoires Bell et le britannique Andrew Steane de l'Université d'Oxford annoncèrent simultanément l'existence de codes quantiques correcteurs d'erreur, ce qui suscita une forte vague d'intérêt pour ce sujet.[9] Jusque là, le concept d'information quantique pouvait en effet apparaître plutôt comme une curiosité théorique, dont les applications potentielles étaient limitées à des processus impliquant un très petit nombre de q-bits. En effet, on sait que des processus irréversibles (comme l'émission spontanée) détruisent rapidement la cohérence quantique et rendent la manipulation d'états quantiques complexes extrêmement difficile. La protection d'états quantiques arbitraires d'un nombre non-négligeable de q-bits au moyen de techniques de correction d'erreur, que l'on croyait inapplicables, devenait soudainement envisageable et ouvrait des perspectives inattendues.

Une première difficulté à appliquer le concept classique de correction d'erreur à un état quantique est liée au fait que toute mesure quantique perturbe apparemment l'état observé. On a déjà vu plus haut que la mesure d'un q-bit dans l'état $(|0\rangle + |1\rangle)/\sqrt{2}$ résulte en un q-bit dans un mélange statistique équiprobable des états $|0\rangle$ et $|1\rangle$. La règle d'or est donc qu'il ne faut pas observer directement le q-bit dans la superposition arbitraire $\alpha|0\rangle + \beta|1\rangle$ que l'on veut protéger, sous peine de le détruire. Une des contributions de Peter Shor fut de remarquer que l'on peut, sous certaines conditions, corriger une erreur sans connaître la valeur du q-bit encodé et donc en préservant toute superposition. Ce phénomène n'a pas d'analogue classique: si un bit encodé à l'aide du code à répétition évoqué ci-dessus résulte par exemple en la chaîne de bits 011, on détecte que le premier bit est erroné, et donc l'on connaît simultanément la localisation de l'erreur et la valeur correcte du bit, c'est-à-dire 1. En mécanique quantique, il est possible, par une mesure partielle, de déterminer précisément l'erreur qui s'est produite sans pour autant acquérir d'information sur le q-bit. Il suffit alors de corriger l'erreur, toujours sans lire le q-bit.

Ensuite, une autre particularité de l'information quantique qu'il faut prendre en compte

[9] A. M. Steane, *Phys. Rev. Lett.*, 77, 793, 1996; P. W. Shor, *Phys. Rev. A*, 52, R2493, 1995.

pour concevoir un code quantique est le rôle de la phase quantique. Un q-bit peut évidemment subir une erreur de type classique, c'est-à-dire une inversion de bit,

$$\begin{aligned}|0\rangle &\rightarrow |1\rangle \\ |1\rangle &\rightarrow |0\rangle\end{aligned}$$

auquel cas la correction d'erreur classique est appliquable. Mais un deuxième type d'erreur qu'il faut également considérer est l'inversion de signe (c'est-à-dire la rotation complexe de la phase quantique par un angle π si le q-bits est dans l'état $|1\rangle$):

$$\begin{aligned}|0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow -|1\rangle\end{aligned}$$

Cette opération est sans équivalent classique puisque la phase quantique n'a pas de signification lors d'une mesure, mais elle altère cependant l'état d'une superposition: par exemple l'état $(|0\rangle + |1\rangle)/\sqrt{2}$ est transformé en l'état distinct $(|0\rangle - |1\rangle)/\sqrt{2}$. Un simplification bienvenue dans le problème de la correction quantique d'erreur provient du fait que toute erreur sur un q-bit peut s'exprimer comme une superposition d'une inversion de bit, d'une inversion de signe, et de leur combinaison c'est-à-dire l'opération

$$\begin{aligned}|0\rangle &\rightarrow |0\rangle \rightarrow |1\rangle \\ |1\rangle &\rightarrow -|1\rangle \rightarrow -|0\rangle\end{aligned}$$

Dès lors, il suffit de vérifier qu'un code corrige séparément une inversion de bit et une inversion de signe en chaque q-bit pour en conclure que toute erreur d'un q-bit est corrigée. Le code de Peter Shor, qui est représenté dans l'encadré ci-contre, est directement inspiré du code à répétition classique mais l'adapte aux spécificités du monde quantique (essentiellement l'existence de l'erreur d'inversion de signe). Ce code permet l'encodage d'un q-bit en neuf q-bits, tel que toute erreur affectant l'un d'eux est corrigeable par l'usage d'un décodeur approprié. L'information quantique (la superposition arbitraire du q-bit encodé) est répartie sur les neuf q-bits de manière à ce que la lecture d'un seul q-bit ne donne aucune information sur la superposition. Seul le décodage des neuf q-bits simultanément permet de localiser et d'identifier une erreur éventuelle, et donc de la corriger, sans avoir à aucun moment mesuré la superposition du q-bit encodé.

La correction d'erreur à l'échelle quantique:

Le code correcteur d'erreur quantique de Peter Shor consiste à encoder un q-bit en neuf q-bits suivant la transformation:

$$
\begin{aligned}
|0\rangle &\rightarrow (|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)\\
|1\rangle &\rightarrow (|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)
\end{aligned}
$$

L'information quantique à préserver (la superposition arbitraire du q-bit encodé) est donc étalée sur les neuf q-bits de sorte que chacun d'entre eux ne détient aucune information (la mesure de chaque q-bit ne révèle qu'un simple mélange statistique équiprobable des états $|0\rangle$ et $|1\rangle$). Il faudrait en fait mesurer un bloc d'au moins trois q-bits pour mesurer (et dès lors détruire!) l'information quantique encodée. Montrons d'abord que ce code est robuste vis-à-vis d'une inversion de bit, par exemple du premier q-bit du premier bloc de trois. La procédure consiste à mesurer la différence (modulo 2) du premier et deuxième q-bit, qui doit être nulle s'il n'y a pas d'erreur. Cette mesure ne détruit pas le q-bit car la différence est constante quelle que soit la superposition encodée. Dans le cas présent, on obtient une différence de 1, ce qui signifie que soit le premier soit le deuxième bit est erroné. Pour distinguer ces deux possibilités, on compare alors le premier et le troisième q-bit de la même manière. Si l'on trouve qu'ils diffèrent, comme dans le cas considéré, c'est le premier q-bit qui est erroné; sinon c'est le deuxième. On peut répéter cette procédure pour chaque bloc de trois q-bits, ce qui permet de localiser l'erreur et de la corriger en effectuant tout simplement une nouvelle inversion du q-bit erroné pour rétablir l'état initial. A aucun moment l'on n'a mesuré le q-bit encodé, ce qui préserve toute superposition.

Bien sûr, une inversion de bit n'est pas le seul type d'erreur. Comme on l'a vu, on peut également avoir une inversion du signe de l'un des q-bits. Si l'un des q-bits du premier bloc subit une telle erreur, les deux états encodés deviennent

$$
\begin{aligned}
|0\rangle &\rightarrow (|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)\\
|1\rangle &\rightarrow (|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)
\end{aligned}
$$

L'astuce est alors d'appliquer une méthode similaire à celle utilisée pour localiser une inversion de bit, mais au niveau des blocs de trois q-bits. Il suffit d'effectuer une mesure particulière des q-bits constituant le premier et le deuxième bloc qui compare les signes de ces blocs. Si l'on détecte qu'ils diffèrent, comme dans la situation présente, on compare alors les signes du premier et du troisième bloc, ce qui permet de localiser l'erreur de signe au niveau du premier bloc. Pour la corriger, il suffit d'inverser à nouveau le signe de la composante $|111\rangle$ du bloc en question. A nouveau, on n'a pas mesuré les signes mais seulement leurs différences de façon a s'assurer qu'ils coïncident.

En bref, le code de Shor exploite la répétition au sein de chaque bloc pour repérer une inversion de bit et la répétition des blocs eux-mêmes pour détecter une inversion de signe. Pour vérifier qu'il protège également contre une erreur du troisième type, il suffit de s'assurer que l'on peut traiter successivement une inversion de bit puis une inversion de signe localisées sur le même q-bit. On en déduit que le code de Shor corrige bien une erreur arbitraire affectant n'importe lequel des neuf q-bits.

La compression de données quantiques

A l'inverse du principe de correction d'erreur, où l'on rajoute de l'information redondante pour obtenir la résistance au bruit, on sait qu'il est possible de comprimer des données si l'on élimine la redondance au sein de celles-ci. Dans ce contexte, une avancée essentielle à cette théorie naissante de l'information quantique est le fait du physicien américain Benjamin Schumacher de Kenyon College, qui a démontré que l'information quantique peut également être comprimée tout comme sa contrepartie classique. Prenons tout d'abord une source classique qui émet l'un des quatre caractères A, B, C, ou D, avec les probabilités respectives 1/2, 1/4, 1/8 et 1/8. Une façon simple de transmettre à un récepteur une séquence générée par la source est de représenter chaque caractère par deux bits: 00 pour A, 01 pour B, 10 pour C, et 11 pour D. Cependant, cette technique n'est pas optimale car la suite de bits obtenue est redondante. Par exemple, un 0 est plus souvent suivi par un autre 0 que par un 1. Une meilleure manière de coder l'information consiste à coder les caractères plus fréquents par une chaîne plus courte: on peut ainsi remplacer le A par 0, le B par 10, le C par 110, et le D par 111. Cela revient à encoder les blocs de 2 bits en une séquence dont la longeur moyenne est de $1 \times \frac{1}{2} + 2 \times \frac{1}{4} + 3 \times \frac{1}{8} + 3 \times \frac{1}{8} = \frac{7}{4}$ bits, soit une économie de 12.5% par rapport à 2 bits. La théorie de Shannon établit que la compression maximale permise est mesurée par l'entropie de la source, c'est-à-dire

$$H = -\sum_i p_i \log_2(p_i)$$

où p_i est la distribution de probabilité des caractères.[10] En général, ce taux de compression est obtenu en codant des blocs de bits de longueur arbitrairement grande. Dans l'exemple présent, le codage de blocs de 2 bits est en fait optimal car l'entropie de Shannon de la distribution est $H(1/2, 1/4, 1/8, 1/8) = 7/4$ bits.

Schumacher a montré que, pour une transmission d'information quantique, c'est l'entropie quantique introduite par von Neumann qui impose une limite sur la compressibilité.[11] Imaginons une source quantique qui produit un photon dont la polarisation est une fois sur deux horizontale (état $|0\rangle$) soit diagonale (état $|a\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$). Aucune redondance classique n'est apparente dans une séquence émise par une telle source puisque les deux symboles sont équiprobables, ce qui semble exclure toute compression. En réalité, le fait que les deux états ne sont pas orthogonaux, et donc pas complètement discernables, induit néanmoins une certaine redondance que l'on peut éliminer en comprimant l'information quantique. La redondance se reflète dans le fait que la matrice de densité représentant le mélange, $\frac{1}{2}(|0\rangle\langle 0| + |a\rangle\langle a|)$, n'est pas proportionelle à la matrice unité et admet les valeurs propres 0.854 et 0.146 (elles devraient valoir 1/2 s'il n'y avait pas de redondance). L'entropie de von Neumann est égale à l'entropie de Shannon de ces valeurs propres et donne $S = H(0.854, 0.146) = 0.601$ bits, ce qui implique que l'économie maximale de photons possible est de 39.9%. En effet, si l'on groupe les photons par blocs de n photons, on peut montrer que la quasi-totalité de l'information quantique est contenue dans un sous-espace qui peut être représenté par un nombre de q-bits qui approche asymptotiquement $0.601 \times n$. Cette technique permet donc de compresser une source arbitraire d'états non-orthogonaux jusqu'à une valeur arbitrairement proche de l'entropie de von Neumann de la source.

[10] L'expression de l'entropie de Shannon montre qu'aucune compression ne peut être appliquée lorsque tous les symboles sont équiprobables, auquel cas H est simplement le logarithme (en base 2) du nombre de caractères.

[11] B. Schumacher, *Phys. Rev. A*, 51, 2738, 1995.

Comment comprimer deux bits classiques en un seul bit quantique grâce à la non-localité quantique?

Une autre singularité de l'information quantique, qui la distingue fondamentalement de l'information classique, est son caractère non-local. L'information classique est toujours locale, ou isolée dans l'espace, dans le sens que la mesure d'un bit localisé en un point révèle totalement la valeur 0 ou 1 de ce bit quelle que soit la valeur d'autres bits en d'autres points de l'espace. Au contraire, deux q-bits peuvent se trouver dans un état corrélé de manière quantique appelé état "intriqué". L'exemple typique d'une situation où deux q-bits ont une "intrication" maximale est l'état quantique dit état EPR après un célèbre article d'Einstein, Podolsky et Rosen datant de 1935.[12] Un tel état, que l'on peut écrire $(|01\rangle - |10\rangle)/\sqrt{2}$, est étonnant à plus d'un titre. La mesure individuelle de chaque q-bit ne révèle rien car on obtient simplement un bit aléatoire (0 ou 1 avec une probabilité égale à 1/2). Toute l'information sur la nature de l'état est répartie sur les deux q-bits à la fois, même s'ils sont séparés par une grande distance. En effet, pour discerner cet état d'une simple juxtaposition de deux q-bits aléatoires non corrélés, il faut les mesurer conjointement dans une base particulière, dite base de Bell en l'honneur du physicien irlandais John Bell. On peut en fait définir trois autres états maximalement intriqués qu'il est impossible de distinguer de cet état EPR si l'on mesure l'un ou l'autre q-bit séparément. On peut néanmoins transformer ces états l'un en l'autre par une simple action sur l'un des q-bits. Ces états forment, avec l'état EPR, la base des états de Bell. Comme ils sont orthogonaux, ces quatre états deviennent à l'inverse parfaitement différenciables si l'on mesure les deux q-bits conjointement, ce qui souligne cet étrange effet de non-localité de l'information quantique (voir encadré sur les manifestations de la non-localité de l'information quantique).

Bien que la non-localité quantique ait été remarquée dès les débuts de la mécanique quantique, en particulier après le célèbre article d'Einstein, Podolsky et Rosen, ce n'est que très récemment que les physiciens ont songé à exploiter cette propriété plutôt que de la "subir" comme une prédiction étrange de la mécanique quantique. La première découverte d'un authentique processus de communication quantique utilisant l'intrication quantique date d'un article de 1992, cosigné par Charles Bennett et Stephen Wiesner.[13] Il s'agit du processus dit de "codage dense", qui permet d'encoder deux bits classiques dans un seul q-bit! Ce processus va à l'encontre de toute intuition, car il semble naturel de penser qu'un système quantique à deux états (un q-bit) ne permette de stocker au maximum qu'un bit d'information (un 0 ou un 1). L'astuce imaginée par Bennett et Wiesner est d'envisager que l'émetteur (Alice) et le récepteur (Bernard) partagent au préalable une paire de q-bits intriqués; chacun d'eux détient l'un des q-bits. Cette intrication quantique s'avère être une ressource additionnelle dont Alice et Bernard peuvent disposer pour accroître le taux de transmission d'un facteur deux. Supposons que la paire de q-bits intriqués soit initialement dans le premier état de Bell, $|B_1\rangle$. Alice voudrait transmettre deux bits classiques (l'une des quatre possibilités 00, 01, 10, ou 11) à Bernard au moyen du q-bit unique qu'elle détient. Pour ce faire, elle commence par effectuer une opération sur ce q-bit qu'elle choisit parmi quatre opérations possibles (l'inversion de bit, de signe, leur combinaison, ou alors simplement laisser le q-bit inchangé) en fonction de la valeur des 2 bits à transmettre. Cette action a pour effet de transformer l'état intrinqué des 2 q-bits en l'un des quatre états de Bell. Comme on l'a déjà vu, ces quatre états ne sont pas différenciables localement, ce qui implique que toute mesure effectuée par Bernard sur l'autre q-bit ne peut donner aucune indication sur les 2 bits classiques. Le contraire serait d'ailleurs en contradiction avec le principe de causalité d'Einstein, puisqu'il permettrait à Alice de communiquer instantanément 2 bits à Bernard! En fait, pour communiquer, il est nécessaire qu'Alice transmette à Bernard

[12] A. Einstein, B. Podolsky et N. Rosen, *Phys. Rev.*, 47, 777, 1935.

[13] C. H. Bennett et S. J. Wiesner, *Phys. Rev. Lett.*, 69, 2881, 1992.

le q-bit qu'elle a manipulé. Bernard peut alors mesurer les 2 q-bits conjointement, ce qui lui permet de distinguer les quatre états de Bell et donc d'inférer la valeur des 2 bits classiques.

Les manifestations de la non-localité de l'information quantique:

Une paire de q-bits corrélés de manière quantique ou "intriqués" peut être décrite par l'un des quatre états de Bell:

$$\begin{aligned} |B_1\rangle &= (|00\rangle + |11\rangle)/\sqrt{2} \\ |B_2\rangle &= (|00\rangle - |11\rangle)/\sqrt{2} \\ |B_3\rangle &= (|01\rangle + |10\rangle)/\sqrt{2} \\ |B_4\rangle &= (|01\rangle - |10\rangle)/\sqrt{2} \qquad \text{(Etat EPR)} \end{aligned}$$

Ces états sont orthogonaux, de sorte qu'une mesure des deux q-bits à la fois permet de distinguer ces 4 états. Toutefois, si les deux q-bits sont mesurés indépendamment, les 4 états donnent le même résultat statistique: 50% de 0 et 50% de 1. Ainsi, ces états apparaissent localement comme identiques. De plus, on peut les transformer l'un en l'autre par une action locale, c'est-à-dire agissant sur l'un des q-bits seulement. Prenons le premier état de Bell, $|B_1\rangle$. Une inversion du signe du deuxième q-bit (lorsque celui-ci est égal à 1) résulte en l'état $|B_2\rangle$, alors qu'une inversion de bit produit $|B_3\rangle$. Enfin, l'action successive de ces deux opérations donne l'état $|B_4\rangle$, ce qui montre que l'on peut obtenir les quatre états de Bell à partir d'un seul. Il faut néanmoins souligner que toute opération effectuée sur l'un des q-bits ne peut être détectée d'aucune façon par une mesure du deuxième q-bit puisque ces états intriqués ne sont pas différenciables localement. Le contraire autoriserait la transmission instantanée d'information, ce qui serait en contradiction avec la théorie de la relativité restreinte d'Einstein.

Considérons l'exemple d'une paire de photons dont les polarisations sont intriquées comme deux q-bits dans le premier des états de Bell, $|B_1\rangle$. La fonction d'onde décrivant ces deux photons est étalée dans l'espace, et correspond donc à une superposition de l'état de polarisation horizontale pour les deux photons ainsi que la composante inverse. Si la mesure de l'un des photons révèle que sa polarisation est horizontale (ou verticale), on peut prédire immédiatement que la mesure de la polarisation du deuxième photon donne le même résultat. Si l'on place un filtre polarisant sur le chemin de chacun des photons, ceux-ci sont soit détectés soit non-détectés tous les deux. En d'autres termes, la direction de polarisation est indéterminée mais identique pour les deux photons. Cependant, même si les polarisations mesurées sont complètement corrélées, la nature de cette corrélation quantique est plus subtile qu'il n'y paraît. Il est en effet incorrect de considérer que les deux photons proviennent d'une source qui génère au hasard des paires de photons horizontaux ou des paires de photons verticaux. Si tel était le cas, un filtre polarisant diagonal disposé sur la trajectoire de chaque photon serait tel que la détection de l'un des photons serait indépendante de la détection du deuxième photon.[a] En fait, on observe que la polarisation mesurée dans cette base diagonale reste corrélée pour les deux photons. Tout se passe comme si la mesure de l'un des photons déterminait immédiatement—et à distance—le résultat de la mesure du deuxième photon, même si cette deuxième mesure est effectuée avant que toute information ne puisse se propager d'un point à l'autre (en admettant que l'information ne peut pas être transmise à une vitesse dépassant celle de la lumière, en accord avec la relativité restreinte d'Einstein). Si l'on analyse finement la statistique des mesures de la polarisation suivant plusieurs orientations de paires de photons intriqués, il est possible de montrer expérimentalement que la mécanique quantique est non-locale.[b]

[a] Un filtre polarisant diagonal placé sur la trajectoire d'un photon de polarisation horizontale ou verticale induit une probabilité de détection de ce photon après le filtre égale à 1/2.

[b] Voir un article de La Recherche sur les inégalités de Bell et l'expérience d'Aspect. Récemment, Nicolas Gisin et son équipe a pu mettre en évidence cette non-localité à une distance de plus de 10 km (W. Tittel et al. Phys. Rev. Lett. 81, 3563, 1998)!

Remarquablement, l'information cachée dans cet unique q-bit est égale à 2 bits puisque Bernard ne peut savoir laquelle des 4 possibilités a été choisie par Alice jusqu'au moment où il reçoit le q-bit. Puisque ce dernier est porté par un support physique (un photon par exemple), il ne peut voyager à une vitesse supérieure à celle de la lumière, et donc la causalité est bien respectée. Une manière d'interpréter ce phénomène est de dire que la paire de q-bits intriqués se décompose en un q-bit d'information virtuelle, détenu à l'avance par Bernard, et un "trou" d'information (−1 bit) pour Alice.[14] Celle-ci code les 2 bits classiques dans le q-bit en comblant ce trou d'information, ce qui résulte en un excès d'un bit (−1+2=1 bit). Lorsque le q-bit est transmis à Bernard et mis en commun avec le deuxième q-bit de la paire initiale, on retrouve les 2 bits classiques. Tout se passe comme si le q-bit détenu initialement par Bernard contenait à l'avance un bit d'information sur ce qui sera encodé par Alice dans le futur! En ce sens, on a donc un transfert d'information à l'envers dans le temps via l'intrication des q-bits, bien que cette étrange propriété de l'information quantique ne viole pas la causalité et, dès lors, ne donne pas lieu à tous les scénarios classiques de science-fiction!

La téléportation quantique n'est plus du domaine de la fiction.

La mise en lumière de ce procédé de codage dense fut suivie de peu par la découverte du principe de la "téléportation quantique" par une équipe de six chercheurs lors du congrès international de l'ISI à Turin en été 1992.[15] Contrairement à ce que son nom indique, la téléportation quantique n'est pas un nouveau mode de transport futuriste, mais bien un processus de communication de l'état arbitraire d'un q-bit (un photon par exemple) qui exploite à nouveau l'intrication entre une paire de q-bits partagés initialement par l'émetteur et le récepteur. Ici, c'est un seul q-bit qui est communiqué au moyen de la transmission de deux bits classiques d'Alice à Bernard, à l'opposé de ce qui se passe pour le codage dense. Alice et Bernard partagent initialement une paire de q-bits intriqués, par exemple dans l'état $|B_1\rangle$. Alice mesure en même temps son q-bit intriqué et le q-bit à communiquer. Elle fait une mesure dans la base de Bell qui peut donner quatre résultats possibles (00, 01, 10, ou 11) puisqu'il y a quatre états de Bell. Elle peut alors transmettre à Bernard les 2 bits obtenus par tout moyen de transmission classique. Lorsque Bernard reçoit ces 2 bits, il effectue l'une des 4 opérations mentionnées ci-dessus sur le deuxième q-bit intriqué, et ce conditionnellement à la valeur des 2 bits. On peut montrer que l'état résultant de ce q-bit coïncide exactement avec l'état initial du q-bit qu'Alice désirait communiquer à Bernard. On a donc un moyen de transmettre de l'information quantique par l'intermédiaire d'information classique, grâce à l'usage de l'intrication quantique. Si les bits classiques sont transmis à la vitesse de la lumière (par onde radio, par exemple), l'information quantique transite également à la même vitesse.

Un lecteur attentif pourrait s'interroger à juste titre sur la possibilité de copier un q-bit en utilisant cette technique de téléportation, ce qui serait en désaccord avec le principe de non-duplication quantique! En effet, à première vue, Bernard détient après la téléportation du q-bit une copie identique à l'original d'Alice. En réalité, on peut voir que l'original doit nécessairement être détruit lorsqu'Alice effectue la mesure de Bell. Il n'y a donc pas de contradiction, et l'information quantique disparait nécessairement de son point de départ avant de réapparaître en un nouveau point de l'espace. De plus, les 2 bits classiques transmis d'Alice à Bernard ne permettent pas d'inférer la moindre information sur la superposition quantique que l'on veut téléporter. De même, le q-bit intriqué que Bernard possède initialement ne contient clairement aucune information puisqu'il existe avant même qu'Alice ne mesure le q-bit inconnu. L'information quantique ne se situe donc apparemment ni dans les 2 bits classiques,

[14] N. J. Cerf et C. Adami, *Phys. Rev. Lett.*, 79, 5194, 1997.

[15] C. H. Bennett et al., *Phys. Rev. Lett.*, 70, 1895, 1993.

ni dans q-bit de Bernard. En revanche, l'étonnant est que la connaissance simultanée des 2 bits classiques et du q-bit permette à Bernard de reconstituer l'état quantique original, bien que son q-bit n'ait jamais interagi directement avec le q-bit détenu initialement par Alice.

Au début de l'année 98, la technique de téléportation quantique a été démontrée expérimentalement presque simultanément par trois équipes, celle de Anton Zeilinger à l'Université d'Innsbruck, celle de Francesco De Martini à l'Université La Sapienza à Rome, et celle de Jeff Kimble au California Institute of Technology. Dans les deux premiers cas, une paire de photons dont la polarisation est intriquée est utilisée, le q-bit téléporté étant la polarisation d'un photon. La troisième expérience concerne la téléportation d'un état quantique continu comme l'amplitude et la phase d'un mode unique du champ électromagnétique. Comme on le voit dans l'encadré ci-contre (la téléportation quantique démontrée), les trois démonstrations expérimentales ont chacune leurs mérites et limites. Nul doute que d'autres expériences viendront encore confirmer ce prodigieux aspect des communications quantiques dans le futur.

La téléportation quantique démontrée: Quand le protocole de téléportation quantique fut proposé, il y a cinq ans, peu de physiciens s'imaginaient qu'une démonstration, même en laboratoire, serait possible avant le siècle prochain. Mais le côté spectaculaire et fascinant de l'entreprise a motivé trois groupes qui ont tous réalisés des prouesses techniques et d'imagination permettant de démontrer que la téléportation quantique n'est pas une chimère. Du point de vue expérimental, la difficulté majeure de ce protocole est la réalisation par Alice de la mesure de Bell (voir l'encadré sur les manifestations de la non-localité de l'information quantique). En effet, cette mesure doit porter à la fois sur le q-bit à téléporter et sur l'un des q-bits intriqués, de telle sorte qu'Alice n'obtienne aucune information ni sur l'un ni sur l'autre des 2 q-bits mesurés, mais uniquement sur leur corrélation quantique (leur état de Bell). Pour réaliser cet exploit, le groupe de Rome[a] a exploité le fait qu'un photon peut porter deux q-bits. Ainsi, le q-bit téléporté et un des deux q-bits intriqués sont portés par le même photon et la mesure de Bell n'implique plus qu'un seul photon. Le groupe d'Innsbruck[b] a lui utilisé 3 photons pour coder en polarisation les 3 q-bits du protocole de téléportation. En fait, pour obtenir 3 photons, le plus simple est de partir de 2 paires de photons (donc de 4 photons), le quatrième photon servant de "trigger". Une difficulté de cette approche est qu'Alice doit effectuer la mesure de Bell sur deux photons provenant de paires différentes. Afin de limiter cette difficulté, une mesure de Bell simplifiée a été utilisée, ne permettant de distinguer qu'un seul des quatre états de Bell. Finalement, le groupe californien[c] n'a pas utilisé une variable discrète, comme un q-bit, mais une variable continue, comme l'amplitude complexe d'un mode du champ électromagnétique. Etonnamment, il est plus facile d'effectuer la généralisation de la mesure de Bell sur de tels systèmes. Par contre, il semble que les distances sur lesquelles cette réalisation du protocole est possible soient plus limitées.

[a] D. Boschi et al., *Phys. Rev. Lett.*, 80, 1121, 1998.
[b] D. Bouwmeester et al., *Nature*, 390, 575, 1997.
[c] A. Furusawa et al., *Science*, 282, 706, 1998.

Nous avons vu que la théorie de l'information de Shannon, qui a débuté dans l'après-guerre comme une théorie mathématique dont l'objet essentiel était de décrire les communications, le codage, ou le cryptage des données, s'est rapprochée singulièrement de la physique au cours de ces dernières années avec les développements d'une théorie quantique de l'information. Les chercheurs ont montré comment de nombreuses notions classiques tels que la compression de données ou la correction d'erreur peuvent être adaptées à l'échelle quantique. D'autres ont mis en évidence les particularités de l'information quantique comme sa résistance à la copie ou la possibilité de téléporter un bit quantique, et l'expérience a permis de confirmer certaines de ces prédictions surprenantes. Tous ces résultats s'ajoutent à la naissance parallèle d'une nouvelle discipline dénommée "informatique quantique" (voir les concepts d'algorithmes quantiques et d'ordinateurs quantiques[16]) et suggèrent que l'on a mis le doigt sur une technique révolutionnaire de traitement de l'information exploitant la cohérence quantique. Même si l'on est extrêmement loin de coder de la "musique quantique" sur des disques compacts de taille atomique, ou, plus sérieusement, de réaliser des hypothétiques ordinateurs quantiques, on assiste certainement aux premiers balbutiements d'une théorie passionante qui tente de cerner la notion d'information à l'échelle atomique, et est en passe de bouleverser notre conception du monde quantique.

Pour en savoir plus:

- Charles Bennett, "Quantum Information and Computation", *Physics Today*, 48, 24, Octobre 1995.
- Andrew Steane, "Quantum Computing", *Report on Progress in Physics*, 61, 117, 1997.
- Colin Williams et Scott Clearwater, "Explorations in Quantum Computing", Springer-Verlag (Telos), 1998.
- Visitez le site Web du réseau européen "The Physics of Quantum Information" soutenu par la Commission Européenne dans le cadre de son programme *Training and Mobility of Researchers*, `http://www.cordis.lu/tmr/src/db087a.htm`

[16]Lire aussi *L'ordinateur sous le charme quantique* dans La Recherche n° 292, novembre 1996.