

AKG-IMAGES

« Plus on fait la chasse aux quantas, mieux ils se cachent. » A. Einstein

Le paradoxe EPR

■ Père fondateur de la physique quantique, Einstein en a ultérieurement rejeté certaines implications. L'impossibilité de prédire les résultats des mesures autrement qu'en termes probabilistes était selon lui la preuve que la théorie quantique était « incomplète », qu'elle oubliait de prendre en compte certains aspects de la réalité.

■ Dans le but de mettre à l'épreuve les principes de la physique quantique, il propose une expérience de pensée, dans un article qu'il cosigne en 1935 avec son jeune assistant, Nathan Rosen, et un autre physicien, Boris Podolsky, qui maîtrise mieux que lui l'anglais. L'argument (dit « EPR », d'après les initiales des auteurs) est le suivant : telles quelles, les lois de la mécanique quantique permettent la formation de paires de particules « intriquées », pour lesquelles la mesure des propriétés de l'une permet de connaître instantanément les propriétés de l'autre, quelle que soit la distance qui les sépare.

■ Pour Einstein, une telle situation est impossible, et la physique quantique ne décrit donc pas correctement la réalité. Niels Bohr pense le contraire, et leur controverse, essentiellement philosophique, restera comme l'une des plus profondes de la physique du xx^e siècle. Une expérience clé a permis de trancher : en 1982, le physicien français Alain Aspect, en s'appuyant sur les travaux de l'irlandais John Bell, a démontré que l'intrication des particules existe effectivement, avec toutes les propriétés annoncées. C.M.

A. Einstein, B. Podolsky et N. Rosen, *Physical Review*, 47, 777, 1935.

L'étrange pouvoir de l'intrication quantique

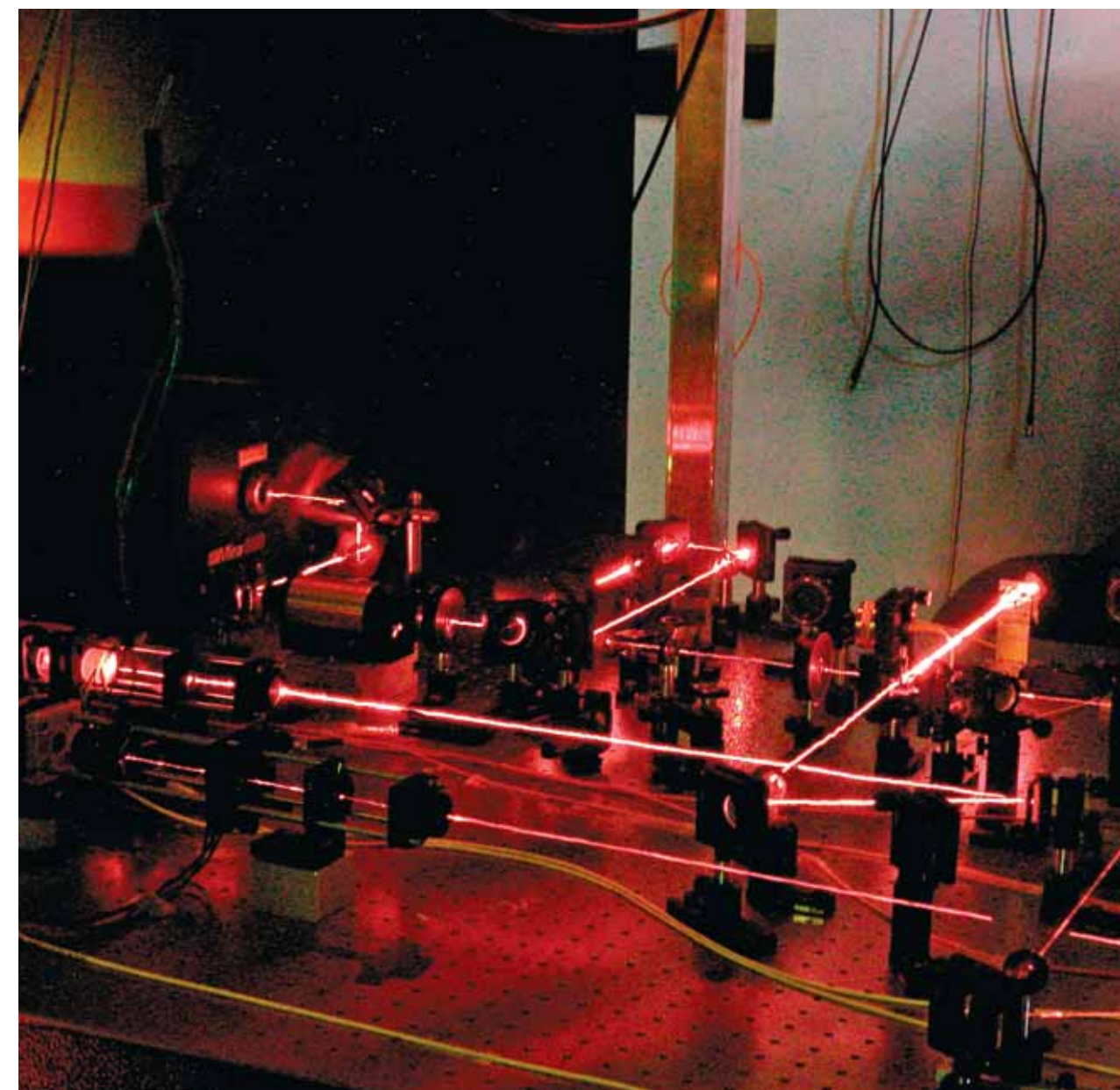
Une expérience de pensée proposée par Einstein pour mettre en défaut la mécanique quantique a conduit, paradoxalement, à l'une des plus fascinantes applications de celle-ci. Grâce à l'intrication quantique, on peut copier parfaitement, et à grande distance, les propriétés d'une particule sur une autre. La téléportation n'est plus de la science-fiction.

Nicolas Cerf est professeur à l'école polytechnique de l'Université libre de Bruxelles, où il dirige le Centre for Quantum Information and Communication. nicolas.cerf@ulb.ac.be

Nicolas Gisin est professeur à l'université de Genève, où il dirige la section d'optique du Groupe de physique appliquée. nicolas.gisin@physics.unige.ch

Notre société a justement été qualifiée de « société de l'information » : les nouvelles techniques de communication, en particulier l'ordinateur et les réseaux informatiques, tel Internet, ont transformé, et transformeront encore, nos manières de vivre. Du codage de la musique sur des disques compacts à la réception des images lointaines des anneaux et des satellites de Saturne observés par la sonde spatiale Cassini, toutes ces réalisations reposent en grande partie sur la théorie mathématique de l'information établie par Claude Shannon peu après la Seconde Guerre mondiale [1]. Malgré ce spectre remarquablement vaste d'applications, Shannon ne soupçonnait sans doute pas que des chercheurs allaient découvrir, quelques décennies plus tard, un prolongement surprenant de ses travaux à l'échelle atomique.

Un premier pas dans cette aventure remonte au début des années 1960, lorsque Rolf Landauer, du laboratoire de recherche d'IBM à Yorktown Heights, défendit l'idée que l'information n'est pas un concept mathématique détaché de toute réalité matérielle : elle est de nature physique, ne serait-ce que parce qu'elle a un support, les molécules d'encre de cette page, la magnétisation des atomes sur un disque d'ordinateur, ou encore le flot d'électrons dans un fil téléphonique. Il n'y a pas d'information sans support physique, et tout procédé de traitement de l'information (stockage, calcul, transmission) est, en définitive, un processus matériel indissociable de la thermodynamique du système physique au sein duquel il se déroule. Landauer montra, en particulier, que l'effacement d'un bit, unité élémentaire d'information à laquelle on attribue



SOURCE DE PHOTONS utilisée dans une expérience de téléportation menée par l'équipe de Nicolas Gisin à l'université de Genève. ©GROUPE DE PHYSIQUE APPLIQUÉE DE L'UNIVERSITÉ DE GENÈVE

conventionnellement les valeurs 0 ou 1, dissipe toujours une quantité minimale d'énergie proportionnelle à la température du support. Aujourd'hui, les supports de l'information que nous manipulons sont des systèmes physiques assez grands, qui

obéissent aux lois de la physique classique : une charge de 10 000 à 100 000 électrons est, par exemple, nécessaire au stockage d'un bit au sein de la mémoire vive d'un ordinateur. Toutefois, pris individuellement, chaque électron a aussi des propriétés phy-

siques mesurables : pourrait-il servir de support à un élément d'information ?

L'information bouleversée

Cette proposition n'est pas un simple exercice intellectuel. D'abord motivés

[1] C.E. Shannon et W. Weaver, *The Mathematical Theory of Communication*, University of Illinois Press, Urbana, 1949.

*La polarisation d'un photon est la direction du champ électrique de l'onde électromagnétique associée.

*La notation $|\psi\rangle$ a été proposée par le physicien britannique Paul Dirac pour écrire le vecteur d'état qui caractérise tout système quantique.

*Une superposition des états $|0\rangle$ et $|1\rangle$ est, de façon générale, notée $\alpha|0\rangle + \beta|1\rangle$, où α et β sont des nombres complexes tels que la somme des carrés de leurs modules est égale à 1 ($|\alpha|^2 + |\beta|^2 = 1$). Si l'on mesure un tel q-bit, on obtient le résultat 0 avec la probabilité $|\alpha|^2$ ou 1 avec la probabilité $|\beta|^2$. Pour alléger les notations, on a omis le facteur $\sqrt{2}$ dans les exemples concernant l'état de polarisation diagonale d'un photon que l'on écrit $|0\rangle + |1\rangle$ au lieu de $(|0\rangle + |1\rangle)/\sqrt{2}$.

par la recherche de traitements de l'information économes en énergie, les physiciens qui se sont intéressés au codage de l'information sur des particules isolées, comme un atome ou un photon, ont rapidement découvert que le concept même d'information en est bouleversé. À cette échelle, ce sont en effet les lois de la mécanique quantique qui s'appliquent. On observe alors des phénomènes étranges. Ils ont en particulier découvert et mis en pratique un concept totalement nouveau, la téléportation quantique. Le terme, popularisé par les scénaristes de la série télévisée *Star Trek* pour désigner un mode de transport par dématérialisation, est passé dans le langage scientifique depuis cette découverte.

Ainsi, comme souvent, la mécanique quantique déjoue l'intuition classique en donnant lieu à des propriétés singulières et totalement insoupçonnées de l'information portée par une particule individuelle. L'état de polarisation* d'un photon peut, par exemple, représenter un « bit quantique », que l'on nomme q-bit. On identifie, de manière conventionnelle, la polarisation horizontale du photon à l'état quantique que l'on note $|0\rangle$, et la polarisation verticale à l'état que l'on note $|1\rangle$ *. À première vue, il n'y a là rien de très différent de la manipulation classique de l'information : si l'on mesure le q-bit en disposant un filtre de polarisation verticale sur la trajectoire du photon, la détection du photon derrière ce filtre sera associée à un 1, alors que sa non-détection équivaudra à un 0.

Superposition d'états

Toutefois, les lois de la mécanique quantique ont une conséquence remarquable : un photon peut être dans un état de polarisation intermédiaire entre la polarisation verticale et horizontale, et la valeur associée au q-bit reste alors indéterminée jusqu'à sa mesure. On décrit un tel état comme la superposition des états de polarisation horizontale et verticale (la manifestation la plus célèbre de ce principe de superposition quantique est le « chat de Schrödinger », qui reste dans un état

intermédiaire entre la vie et la mort tant que l'on n'a pas ouvert la boîte où il est enfermé, lire l'article de Serge Haroche, Jean-Michel Raymond et Michel Brune, p. 76). Un q-bit décrit de cette manière n'a pas d'analogue classique : un bit classique est soit un 0, soit un 1, mais jamais un état intermédiaire. Si l'on mesure un q-bit dans un état de superposition, on a une certaine probabilité d'obtenir la valeur 0 et une autre probabilité d'obtenir la valeur 1, la somme des deux probabilités étant égale à 1 [fig. 1].

Ainsi, un q-bit associé à un photon qui se trouve dans un état de polarisation diagonale (dont l'orientation fait un angle de 45 degrés avec l'horizontale) peut être interprété comme étant dans une superposition* uniforme des états de polarisation horizontale et verticale, notée $|0\rangle + |1\rangle$. Si un filtre polarisant vertical est placé sur la trajectoire du photon, la probabilité que ce dernier

Une caractéristique fondamentale de l'information quantique est sa non-localité.

soit détecté en aval (donc que l'on obtienne la valeur 1) est de 1/2, tout comme la probabilité que le photon ne soit pas détecté (et que l'on obtienne la valeur 0). Toutefois, le q-bit dans l'état $|0\rangle + |1\rangle$ n'est pas une sorte de bit aléatoire, comme s'il résultait du tirage au hasard de boules portant les chiffres 0 ou 1. En effet, on détecte toujours le photon de polarisation diagonale en aval d'un filtre polarisant diagonal, tandis qu'un photon polarisé horizontalement ou verticalement ne serait détecté qu'avec une probabilité de 1/2 derrière un filtre polarisant diagonal : l'état $|0\rangle$ ou $|1\rangle$ est une superposition uniforme des états de polarisation diagonale ($|0\rangle + |1\rangle$) et antidiagonale ($|0\rangle - |1\rangle$). Ce principe de superposition rend le traitement de l'information quantique très différent de celui de l'information classique. Cet effet est d'autant plus

spectaculaire lorsqu'on l'associe avec une autre caractéristique de l'information quantique, sa non-localité : deux q-bits peuvent être corrélés de manière quantique et le rester, même s'ils empruntent des chemins différents et s'éloignent l'un de l'autre. Au contraire, l'information classique est locale : la lecture d'un bit localisé en un point de l'espace est indépendante des bits présents en d'autres points.

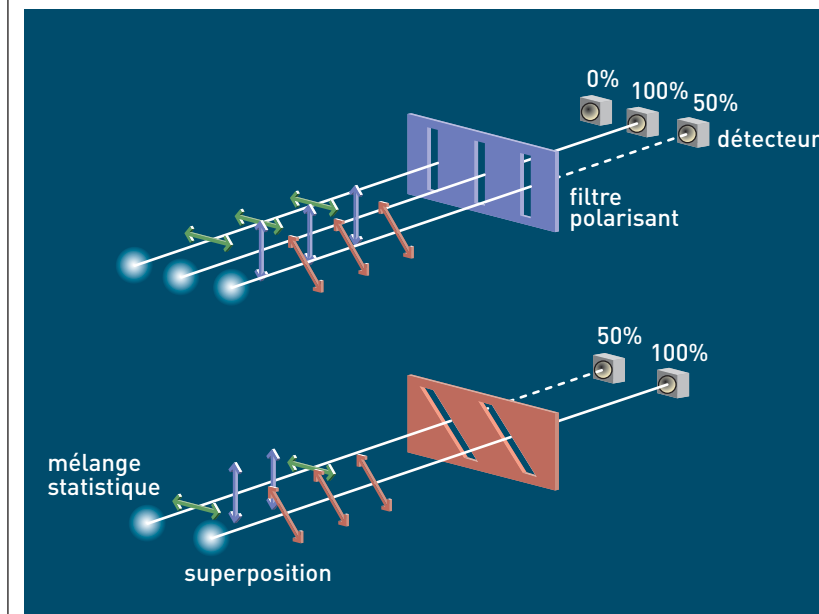
Photons intriqués

L'illustration typique de la non-localisation est le cas où deux q-bits sont portés par une paire de photons dits « intriqués », produits simultanément par un même processus physique et décrits par une seule fonction d'onde de la forme $|0\rangle_x |1\rangle_y - |1\rangle_x |0\rangle_y$. Dans cet état quantique particulier, décrit sous une forme analogue par Einstein, Podolsky et Rosen [2], en 1935, la mesure individuelle de l'état d'un seul q-bit ne révèle rien : on obtient seulement 0 ou 1 avec une probabilité égale à 1/2. En revanche, on peut immédiatement prédire que la mesure de l'autre q-bit donnera le résultat opposé,

quelle que soit la distance qui sépare les deux photons au moment de la mesure. Même si cet état intriqué ressemble à celui de deux q-bits aléatoires simplement corrélés, la nature de cette « intrication » quantique est plus subtile qu'il n'y paraît : toute l'information sur l'état de la paire est répartie sur les deux q-bits à la fois.

Plus généralement, on peut définir quatre états intriqués particuliers, nommés « états de Bell »*, qui ont cette même propriété. On ne peut pas les distinguer les uns des autres si l'on ne mesure que l'un des deux q-bits de la paire, car une telle mesure résulte toujours en un bit aléatoire, comme on l'a vu ci-dessus. En revanche, la mesure conjointe des deux q-bits, nommée « mesure de Bell », suffit à la détermination sans ambiguïté de l'état dans lequel se trouvait la paire. En outre, une

Fig.1 Une superposition quantique est distincte d'un mélange statistique



EN MÉCANIQUE QUANTIQUE, L'ÉTAT D'UNE PARTICULE INDIVIDUELLE peut être une superposition de deux états. Par exemple, l'état de polarisation diagonale d'un photon ($|0\rangle + |1\rangle$, en orange) est la superposition d'un état de polarisation horizontale ($|0\rangle$, en vert) et d'un état de polarisation verticale ($|1\rangle$, en violet) : des photons polarisés diagonalement sont détectés une fois sur deux derrière un filtre de polarisation verticale. Cette superposition diffère d'un mélange statistique de photons polarisés verticalement et horizontalement : la moitié seulement des photons d'un tel mélange est détectée derrière un filtre de polarisation diagonal, tandis que tous les photons polarisés diagonalement sont détectés derrière un tel filtre (en bas).

action simple sur un seul des q-bits (inversion de bit, inversion de signe* ou combinaison des deux) transforme de façon univoque chacun de ces états de Bell en l'un des trois autres. C'est cette dernière propriété qu'ont exploitée Charles Bennett, d'IBM, et Stephen Wiesner, pour proposer, en 1992, un processus de communication quantique utilisant l'intrication de q-bits [3]. Leur « codage dense » permet l'encodage (et l'échange) de deux bits classiques en un seul q-bit. Il s'agit là d'un processus qui va à l'encontre de toute intuition classique : comment un système quantique à deux états, le $|0\rangle$ et le $|1\rangle$, peut-il contenir plus d'un bit d'information? Supposons que deux personnes nommées Alice et Bernard souhaitent échanger des informations en utilisant ce procédé. Préalablement à la commu-

nication, ils se partagent une paire de q-bits intriqués, préparée dans un état de Bell fixé à l'avance. Lorsque Alice souhaite transmettre deux bits à Bernard, elle transforme le q-bit qu'elle détient à l'aide de l'une des quatre opérations possibles (l'inversion de bit, l'inversion de signe, leur combinaison, ou simplement la conservation du q-bit original) en fonction de la valeur des deux bits, afin que la paire se trouve désormais dans l'état de Bell correspondant à ses deux bits. Pour ce faire, Alice et Bernard ont associé à l'avance chacun des quatre états de Bell avec l'une des quatre chaînes possibles de deux bits (00, 01, 10, 11). Ensuite, Alice transmet à Bernard le q-bit qu'elle a manipulé. Il suffit alors à Bernard de mesurer conjointement les deux q-bits de la paire, afin de savoir dans quel état

de Bell celle-ci se trouve, et donc de connaître la valeur des deux bits qu'Alice souhaitait lui communiquer.

De façon remarquable, l'information cachée dans cet unique q-bit transmis est donc égale à deux bits. Il s'agit bien d'une transmission d'information puisque, même si Bernard possède l'alter ego du q-bit d'Alice, il ne peut savoir laquelle des quatre possibilités a été choisie par Alice qu'au moment où il reçoit le q-bit qu'elle détenait. L'intrication quantique augmente ainsi le taux de transmission d'un facteur deux. Une manière d'interpréter ce phénomène est de considérer 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) détenu par Alice [4]. En codant les deux bits classiques dans son q-bit, Alice comble ce trou d'information et hérite d'un bit en excès (-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 deux bits classiques. Tout se passe donc comme si le q-bit détenu initialement par Bernard contenait à l'avance un bit d'information virtuelle sur ce qui sera encodé par Alice dans le futur. Cependant, aussi étrange soit-elle, cette propriété ne viole pas le principe de causalité énoncé par Einstein : Bernard ne possède aucune information sur la valeur des deux bits tant qu'il n'a pas reçu le q-bit d'Alice qui, porté par un support matériel, par exemple un photon, ne peut pas être transmis instantanément. Une version simplifiée de ce protocole a d'ailleurs été vérifiée expérimentalement en 1996 [5].

Annnonce scientifique

L'exposé de ce procédé de codage dense fut suivi de peu par la découverte de la « téléportation quantique », annoncée au cours de l'été 1992 par une équipe de six chercheurs participant au congrès de l'Institut pour l'échange scientifique de Turin [6]. En dépit de son nom, la téléportation quantique n'est pas un nouveau mode de transport futuriste : elle est limitée à la communication de

*L'inversion de signe d'un q-bit correspond à la rotation d'un angle de 180° (dans le plan complexe) de la phase quantique de l'état $|1\rangle$. Toute particule possède une phase quantique qui donne lieu à des propriétés ondulatoires, par exemple les interférences qui se manifestent dans une expérience de diffraction d'électrons. Un q-bit est donc caractérisé par une phase quantique, qui perd sa signification une fois la mesure effectuée et n'a pas d'analogue en théorie classique de l'information.

- [2] A. Einstein, B. Podolsky et N. Rosen, *Phys. Rev.*, 47, 777, 1935.
[3] C.H. Bennett et S.J. Wiesner, *Phys. Rev. Lett.*, 69, 2881, 1992.
[4] N.J. Cerf et C. Adami, *Phys. Rev. Lett.*, 79, 5194, 1997.
[5] K. Mattle et al., *Phys. Rev. Lett.*, 76, 4656, 1996.

* Les états de Bell, ainsi nommés en l'honneur du physicien irlandais John Bell, sont de la forme $|0\rangle|x\rangle|0\rangle + |1\rangle|x\rangle|1\rangle$, $|0\rangle|x\rangle|0\rangle - |1\rangle|x\rangle|1\rangle$, $|0\rangle|x\rangle|1\rangle + |1\rangle|x\rangle|0\rangle$, et $|0\rangle|x\rangle|1\rangle - |1\rangle|x\rangle|0\rangle$.

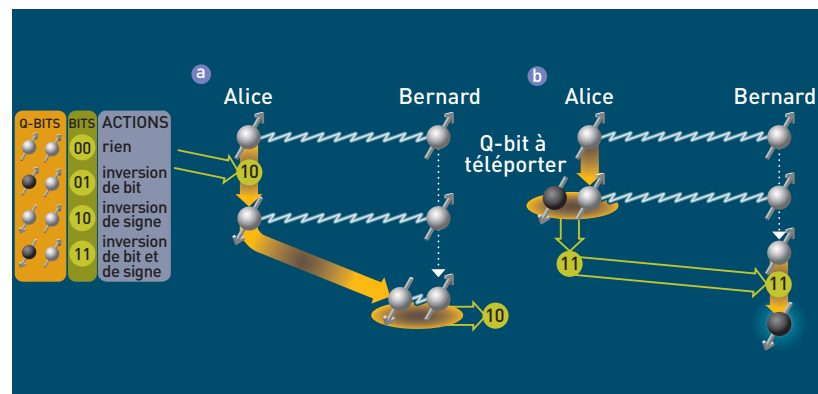
l'état d'un q-bit par l'échange de deux bits classiques.

Principe de causalité

Comment téléporter un q-bit? Comme pour le codage dense, Alice et Bernard partagent initialement une paire de q-bits intriqués dans un état de Bell connu. Alice mesure simultanément son q-bit intriqué et le q-bit à téléporter : le résultat est l'un des quatre états de Bell*. Elle peut alors transmettre à Bernard la chaîne de deux bits classiques correspondante par un moyen quelconque de communication classique : ces deux bits indiquent à Bernard laquelle des quatre opérations il doit réaliser sur son propre q-bit intriqué pour que l'état résultant de celui-ci coïncide exactement avec l'état initial du q-bit qu'Alice voulait téléporter. L'usage de l'intrication quantique rend donc possible la transmission d'information quantique par l'intermédiaire de bits classiques. À nouveau, le principe de causalité n'est pas remis en cause par ce scénario, car la téléportation du q-bit n'est pas instantanée : les deux bits classiques sont transmis au mieux à la vitesse de la lumière, qui a une valeur finie.

De plus, les deux bits classiques transmis d'Alice à Bernard ne donnent, à

Fig.2 Codage dense et téléportation



L'INTRICATION QUANTIQUE, SOURCE DE PARADOXES, À DES APPLICATIONS PRATIQUES. En mécanique quantique, deux particules peuvent être « intriquées » : elles restent interdépendantes quelle que soit la distance qui les sépare ; l'état de la paire (parmi quatre états de Bell possibles) ne peut être déterminé que par la mesure simultanée des deux particules (la mesure dite « de Bell »). Le partage d'une paire de q-bits dans un état de Bell connu permet à Alice et Bernard d'échanger des informations, grâce à la correspondance entre les quatre états de Bell et chacune des quatre chaînes de deux bits possibles, et grâce à la possibilité qu'ils ont de passer de l'un de ces états de Bell à un autre par une action sur un seul des q-bits. Ainsi, dans le codage dense (a), Alice modifie son q-bit de façon que l'état de la paire corresponde à deux bits qu'elle souhaite transmettre (ici, par exemple, 10). Puis elle envoie ce q-bit modifié à Bernard qui, en mesurant les deux q-bits simultanément, en déduit l'état de la paire, donc la valeur des deux bits. La téléportation (b) est le scénario symétrique : Alice mesure, par une mesure de Bell, son q-bit intriqué et le q-bit à téléporter, et en déduit deux bits (ici, par exemple, 11), qu'elle envoie à Bernard. Celui-ci n'a plus qu'à modifier son q-bit en fonction des deux bits reçus d'Alice : son q-bit se retrouve alors exactement dans le même état que le q-bit d'Alice.

LA TÉLÉPORTATION QUANTIQUE DÉMONTRÉE

Trois équipes ont réussi à démontrer expérimentalement le principe de téléportation quantique, en 1997. Du point de vue expérimental, la principale difficulté de la téléportation quantique est la réalisation par Alice de la mesure simultanée du q-bit qu'elle souhaite téléporter et du q-bit intriqué qu'elle possède (mesure de Bell), de telle sorte qu'elle n'obtienne aucune information ni sur l'un ni sur l'autre des deux q-bits mesurés, mais uniquement sur leur corrélation quantique.

Pour réaliser cet exploit, le groupe de Francesco De Martini, de l'université de Rome, a exploité le fait qu'un photon peut porter deux q-bits [7] : le q-bit téléporté et l'un des deux q-bits intriqués. Dans ce cas, la

mesure de Bell n'implique plus qu'un seul photon, ce qui simplifie l'expérience. Le groupe d'Anton Zeilinger, de l'université d'Innsbruck, a utilisé trois photons pour coder en polarisation les trois q-bits intervenant dans le procédé de téléportation [8]. Le plus simple est de partir de deux paires intriquées, donc de quatre photons, et de n'en utiliser que trois, le quatrième servant pour la synchronisation. Une difficulté de cette approche est qu'Alice doit alors effectuer la mesure sur deux photons provenant de paires différentes. Afin de surmonter cette difficulté, une mesure simplifiée a été utilisée, ne permettant de distinguer qu'un seul des quatre états de Bell.

Enfin, le groupe de Jeff Kimble, de l'Institut de technologie de Californie, n'a pas utilisé une variable discrète, comme un q-bit, mais une variable continue : l'amplitude complexe d'un mode du champ électromagnétique [9]. Il est en effet plus facile d'effectuer la généralisation de la mesure de Bell sur de tels systèmes. En revanche, il semble que les distances sur lesquelles cette réalisation du protocole est possible soient intrinsèquement limitées. Ces trois expériences ont ensuite stimulé de nombreux travaux, et aujourd'hui la téléportation d'un q-bit de lumière via une fibre optique [10] ou encore la téléportation d'un q-bit atomique [11] sont devenues des réalités expérimentales.

eux seuls, aucune information sur l'état du q-bit qu'Alice veut téléporter, car le contraire perturberait nécessairement celui-ci. D'ailleurs, le q-bit intriqué que Bernard possède initialement ne contient pas non plus d'information puisqu'il existe avant même qu'Alice ne mesure le q-bit inconnu. L'information quantique ne se situe donc ni dans les deux bits classiques ni dans le q-bit de Bernard. Seule leur connaissance simultanée permet à Bernard de reconstituer l'état quantique original, bien que son q-bit n'ait jamais interagi directement avec le q-bit qu'Alice veut téléporter.

Quand cette technique de téléportation quantique fut proposée, en 1992, peu de physiciens imaginaient qu'une démonstration expérimentale serait possible rapidement. Toutefois, le côté spectaculaire et fascinant de l'entreprise était tel que, dès la fin de 1997, trois équipes

indépendantes sont parvenues à vérifier expérimentalement, et de façon presque simultanée, la téléportation quantique (voir l'encadré « La téléportation quantique démontrée », p. 88).

Nouveaux horizons

Ces réalisations ne sont sans doute qu'un avant-goût des développements qui pourraient, dans le futur, exploiter ce prodigieux aspect des communications quantiques. On est encore loin de coder de la « musique quantique » sur des disques compacts de taille atomique ou, plus sérieusement, de réaliser un hypothétique ordinateur quantique [1]. Toutefois, on assiste aux premiers balbutiements d'une théorie passionnante de l'information quantique, qui ouvre de nouveaux horizons, totalement insoupçonnés au regard des principes classiques de traitement de l'information. Des lois quantiques, autre-

fois vues seulement comme sources de paradoxes, et des énoncés formulés dans le but même de mettre en défaut la mécanique quantique deviennent ainsi des outils permettant de réaliser des opérations sans équivalent classique au niveau des quanta d'information. ■

N.C. et N.G.

POUR EN SAVOIR PLUS

- ▷ C.H. Bennett, G. Brassard, A.K. Ekert, *Scientific American*, 267, 50, 1992.
- ▷ C.H. Bennett, *Physics Today*, 48, 24, 1995.
- ▷ A. Steane, *Report on Progress in Physics*, 61, 117, 1997.
- ▷ A. Zeilinger, *Physics World*, 11, 3, 1998.
- ▷ G. Alber et al., *Quantum information : An introduction to basic theoretical concepts and experiments*, Springer Tracts in Modern Physics, Vol 173, Springer, Berlin, 2001.

www.larecherche.fr

La Recherche a publié : [1] A. Barenco, A. Ekert, C. Macchiavello et A. Sanpera, « L'ordinateur sous le charme quantique : un saut d'échelle pour les calculateurs », *La Recherche*, novembre 1996.

Cet article est la version revue et mise à jour par ses auteurs du texte paru dans le numéro 327 de *La Recherche*.