

Enfin, après 2015, toute une série d'expériences ont emporté l'assentiment de la communauté scientifique. Des techniques plus performantes ont apporté des solutions à toutes ces failles et la probabilité que les résultats observés soient compatibles avec les deux principes classiques est extrêmement faible. Elle a été estimée à moins de 1 sur 10^{28} pour l'une des expériences ! L'impossibilité de concilier la mécanique quantique avec le principe de localité (ou avec l'indépendance du choix de la mesure) ne fait aujourd'hui plus aucun doute.

DES APPLICATIONS QUANTIQUES

Les physiciens n'ont pas attendu ces dernières réalisations expérimentales pour explorer les possibilités offertes par la non-localité quantique. Loin de se limiter à la seule compréhension théorique du phénomène, ils ont mis à profit celui-ci dans diverses applications.

Il est par exemple possible d'utiliser la non-localité quantique pour obtenir des générateurs de nombres fondamentalement aléatoires. Avec des systèmes classiques, on ne peut que simuler un comportement aléatoire, et les nombres produits ne sont que « pseudoaléatoires ». Or un générateur de nombres aléatoires est une ressource cruciale en informatique, pour les algorithmes d'optimisation, pour la sécurité informatique ainsi que pour les jeux de hasard. En matière de sécurité, il est aussi possible d'utiliser la non-localité quantique pour certifier le bon fonctionnement de dispositifs quantiques, c'est-à-dire pour garantir l'absence d'une faille exploitable par un attaquant. Et cette certification peut être réalisée même dans le cas où les dispositifs ont été fabriqués ou manipulés par une personne à qui l'on ne peut accorder une totale confiance.

La non-localité quantique est aussi à l'origine de protocoles cryptographiques dans lesquels un message échangé est sécurisé contre « toute attaque » (chose impossible dans le monde classique). Cette volonté de sécuriser les communications prend la forme d'un internet quantique où le réseau serait fondé sur l'échange de photons intriqués. Par rapport aux expériences de Bell qui utilisent une unique source de photons, comme dans GHZ, un tel réseau est un immense défi technique. Il n'est pas possible de concevoir une source émettant des photons intriqués pour un grand nombre d'utilisateurs. En outre, par essence, internet est un réseau décentralisé. L'idée est donc d'utiliser plusieurs sources indépendantes de photons intriqués, chacune reliant deux nœuds du réseau.

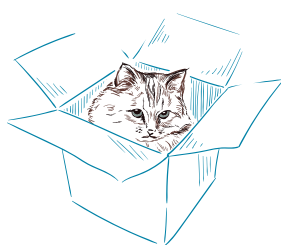
D'un point de vue de l'analyse théorique, ces systèmes quantiques à plusieurs sources indépendantes sont radicalement différents de GHZ ou CHSH. La question qui se pose est

alors de savoir ce que devient la non-localité dans cette situation. Pour l'étudier, les chercheurs ont commencé par examiner les réseaux les plus simples possible.

Intéressons-nous d'abord au cas du réseau « simple » en triangle. Dans l'expérience quantique concrète, on a toujours trois chercheuses, mais la source est remplacée par trois sources indépendantes placées sur chaque côté du triangle (voir la figure page 36). Chaque physicienne mesure cette fois ce qui lui est envoyé par deux sources distinctes afin d'obtenir son résultat. Ainsi, Aïda reçoit deux chats quantiques, et procède à une certaine mesure faisant intervenir les deux félins (par exemple, elle peut examiner la parité des mesures de couleurs, c'est-à-dire le fait d'avoir deux couleurs identiques ou deux différentes) pour obtenir son résultat. Béatrice et Camélia font de même.

Imaginons de nouveau que le détective soit face à une telle expérience et qu'il tente de l'expliquer au moyen de son intuition classique. Le détective voit toujours des corrélations et ne connaît pas le fonctionnement interne de l'expérience. Comme pour l'expérience GHZ, il fait une première déduction

LE CHAT DE SCHRÖDINGER, LA BARRIÈRE DES MOTS



Une difficulté en physique quantique est de traduire des phénomènes observés avec des mots. Le chat de Schrödinger et ceux de l'expérience GHZ en sont un bon exemple. Lorsqu'un individu (un détective) essayait d'interpréter cette dernière expérience selon sa vision classique, il va y plaquer son intuition macroscopique et son vocabulaire. Ainsi, dans son raisonnement, quand un chat emprunte un des tunnels de l'expérience, le pelage, à ce

moment, est vert ou rose (il s'agit ici d'un « ou » exclusif). On parle de principe de réalisme : la couleur du pelage étant une propriété mesurable, valant soit vert soit rose, tout pelage a, à tout moment, une couleur bien définie, verte ou rose.

En physique quantique, ce type de raisonnement n'est plus valide. La couleur du pelage d'un chat quantique est mesurable, mais se demander quelle est cette couleur lorsque celui-ci passe dans le tunnel n'a pas de sens : la couleur n'a pas de réalité tant qu'elle n'est pas mesurée. Concrètement, il n'est plus possible de raisonner comme le fait le détective, en considérant successivement toutes les couleurs possibles. Il faut donc inventer un nouveau mot pour caractériser la propriété « couleur du pelage » avant qu'elle ne soit mesurée. Le mot « ou » étant déjà utilisé, les physiciens emploient le mot « et ». Celui-ci a l'avantage de n'avoir encore aucun sens dans ce contexte. On écrit donc que le pelage du chat empruntant le tunnel est vert et rose. C'est le même mot « et » que l'on retrouve dans le célèbre exemple du chat de Schrödinger dans sa boîte : ce chat est « mort et vivant », car il peut être retrouvé mort ou vivant en ouvrant la boîte, mais il n'est pas, avant l'ouverture, mort avec une certaine probabilité ou vivant avec la probabilité complémentaire. Ainsi, ce mot et n'a de sens que parce qu'il s'oppose au mot ou. On utilise aussi les termes d'« intrication » et de « superposition », en écrivant que la couleur est intriquée dans une superposition des états rose et vert.

Le chat de Schrödinger, mort et vivant dans sa boîte, est une image de ce qui peut être lu dans le formalisme de la physique quantique (lequel donne une caractérisation plus précise et quantitative de ce que signifie le « et »). L'expérience de Bell va plus loin. Elle montre qu'un raisonnement classique à partir du seul mot « ou » est incohérent avec les observations. Elle prouve que le mot « et » est obligatoire pour expliquer l'expérience.

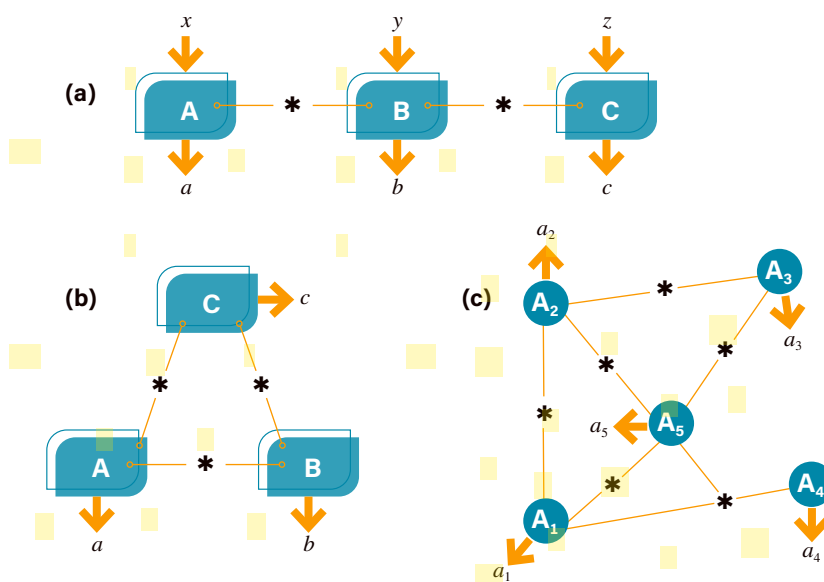
identique: les corrélations doivent s'expliquer par une cause – ou une source – unique. Notons que le détective n'a aucune raison de limiter le nombre de chats émis par cette source: ici, pour coller aux observations, il imaginera une source unique qui émet une «paire de chats» vers chacune des scientifiques. Ainsi, la topologie de l'expérience imaginée par le détective devient différente de la topologie réelle de l'expérience.

Pour éviter cette différence, nous choisissons en quelque sorte d'aider le détective en lui indiquant la topologie de l'expérience et le fait que les corrélations proviennent d'un réseau constitué de trois sources indépendantes disposées en triangle. Il doit alors chercher un raisonnement compatible avec la localité, l'indépendance du choix de la mesure et la topologie expérimentale pour expliquer les résultats des chercheuses. Cette topologie du réseau triangulaire impose de nouvelles contraintes qui réduisent drastiquement le nombre d'explications possibles pour le détective. Ainsi, connaissant la topologie en triangle, il y a davantage de raisons d'arriver à une contradiction.

LE DÉFI DES RÉSEAUX

Pour le détective, le problème devient pourtant beaucoup plus difficile à analyser. La raison est mathématique: avec une source unique, les trois scientifiques peuvent se coordonner. Par exemple, imaginons qu'elles ont à leur disposition une première expérience fondée sur une première source de chats, mesurés d'une certaine façon, et une seconde expérience utilisant une seconde source de chiens, mesurés d'une autre manière. Il leur est possible de créer une troisième expérience à partir de ces deux premières, où une nouvelle source construite à partir des deux précédentes envoie tantôt les chats de la première source, tantôt les chiens de la seconde et un signal indiquant aux scientifiques s'il faut cette fois-ci mesurer des chats ou des chiens. Cette possibilité de coordination implique que la structure de l'espace des explications possibles est «convexe». Cette propriété permet une exploration assez simple de toutes les stratégies possibles, et ainsi de démontrer que l'expérience observée par le détective est nécessairement non locale.

Dans le cas de trois sources indépendantes, ce type de coordination est totalement impossible: dans un réseau en triangle, à partir d'une première expérience avec des chats, et d'une seconde avec des chiens, il est impossible d'en créer une nouvelle où les chats et les chiens alternent (il arrivera toujours un moment où une source enverra des chats, et une autre des chiens, simultanément). Ainsi, le problème n'est plus convexe: malgré un plus faible nombre de stratégies possible, les explorer toutes devient très difficile. C'est toute la



difficulté pour les spécialistes de la non-localité en réseau: pour une topologie donnée, quelle expérience (ou stratégie) est non locale, et comment le démontrer?

Depuis une dizaine d'années, les physiciens imaginent des exemples concrets d'expériences afin de mieux comprendre cette nouvelle forme de non-localité en réseau. En 2010, Cyril Branciard, maintenant à l'institut Néel, à Grenoble, et ses collègues (dont l'un de nous, Nicolas Gisin) ont envisagé un nouveau type d'expériences quantiques, dites de «bilocalité», qui utilisent deux sources indépendantes (voir la figure ci-dessus). L'équipe a imaginé une expérience en partant de cette topologie et a montré que les résultats attendus des mesures étaient inexplicables pour le détective. Cette expérience est un premier pas vers un réseau à plusieurs sources. Cependant, on constate que les corrélations restent ici analogues à celles des expériences de type Bell. Autre limite: dans un réseau purement quantique, on voudrait que les mesures soient intriquées. Il s'agit d'une sorte de parallèle avec le chat dans un état «mort et vivant» (voir l'encadré page 38), mais appliqué aux appareils de mesure, où l'on pourra dire qu'un photon est «mesuré venant de la gauche et de la droite».

La recherche d'autres exemples a mené les physiciens à se tourner vers le réseau en triangle. En 2012, Tobias Fritz, alors à l'institut des sciences photoniques de Barcelone, a fait une première découverte importante. En s'inspirant de l'expérience de Bell standard CHSH, qui fait intervenir deux scientifiques uniquement, il est parvenu à construire un premier exemple de non-localité quantique dans le réseau en triangle. En pratique, dans l'expérience CHSH, Aïda et Béatrice sont équipées de générateurs de nombres aléatoires (remplaçant les pièces pour tirer à pile ou face). L'idée

La topologie des systèmes en réseau comportant plusieurs sources de photons indépendantes devient très riche. Dans l'expérience de bilocalité (a), on utilise deux sources de photons entre trois observateurs. L'observateur B réalise une mesure simultanée sur les deux photons qu'il reçoit. Dans le réseau en triangle avec trois sources (b), chacun des trois observateurs reçoit deux photons. Ces réseaux sont déjà complexes à étudier, mais l'internet quantique contiendra bien plus de sources indépendantes (c, un réseau avec seulement six sources)!