

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.

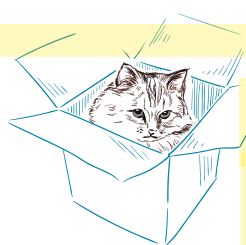
D'un point de vue de l'analyse théorique, ces systèmes quantiques à plusieurs sources indépendantes sont radicalement différents de GHZ ou CHSH. La question qui se pose est

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) essaye 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.