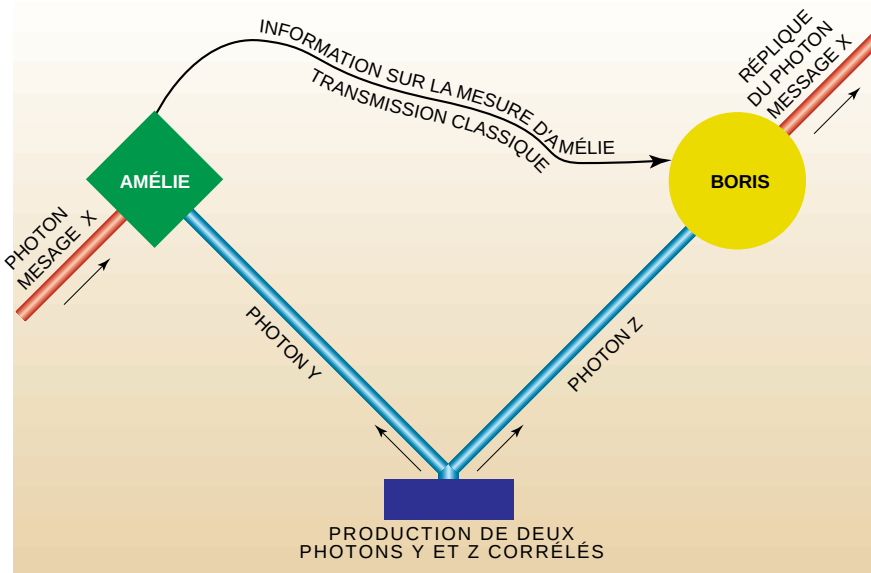




3. LA TÉLÉPORTATION QUANTIQUE est un moyen de faire voyager de l'information inconnue (un état quantique) à la vitesse de la lumière. Amélie veut transmettre l'état quantique d'un photon X à Boris. Elle ne peut prendre totalement connaissance de cet état quantique et doit quand même le communiquer par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

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

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

et les expériences de calcul quantique de ces derniers mois ont confirmé les prévisions des modèles théoriques.

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

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

La téléportation

Il n'en est rien : la technique de téléportation, proposée en 1993 par C. Bennett, G. Brassard, C. Crépeau,

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

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

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

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

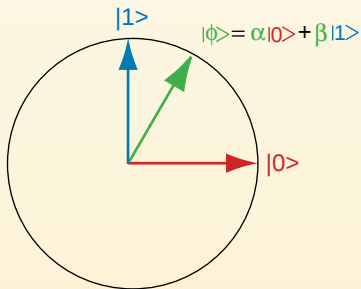
La téléportation quantique pourrait devenir utile, car elle est en mesure de régler le problème qui fait que la cryptographie quantique ne peut fonctionner que sur des distances limitées

a)



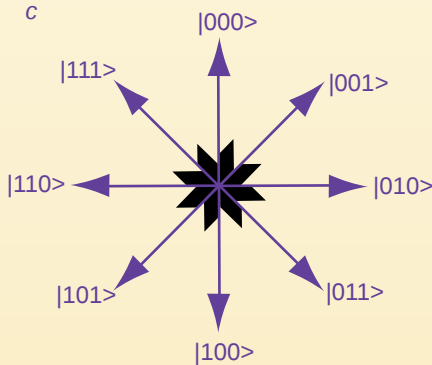
a) L'information unitaire classique est le bit : un objet qui vaut 0 ou 1.

b)



b) L'information unitaire quantique est le qubit (quantum bit). C'est un vecteur dans un espace complexe de dimension 2 muni d'un produit scalaire (deux vecteurs dont le produit est nul sont orthogonaux). Les éléments d'une base orthogonale sont fixés et notés $|0\rangle$ et $|1\rangle$. Un qubit $|\phi\rangle$ se représente sous la forme $\alpha |0\rangle + \beta |1\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$, où α et β sont des nombres complexes (ainsi le qubit est déterminé par quatre nombres réels). Une mesure amène le qubit $|\phi\rangle$ sur l'un des vecteurs de la base $|0\rangle$, $|1\rangle$. Les règles de la mécanique quantique indiquent qu'on obtient, lors d'une mesure physique, $|0\rangle$ avec la probabilité $|\alpha|^2$ et $|1\rangle$ avec la probabilité $|\beta|^2$.

c)



c) L'état quantique d'un N-qubit est un vecteur dans un espace analogue à celui du qubit, mais de dimension 2^N . On choisit une base orthogonale de cet espace.. Pour un 3-qubit on choisit une base orthogonale dont les vecteurs sont : $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$.

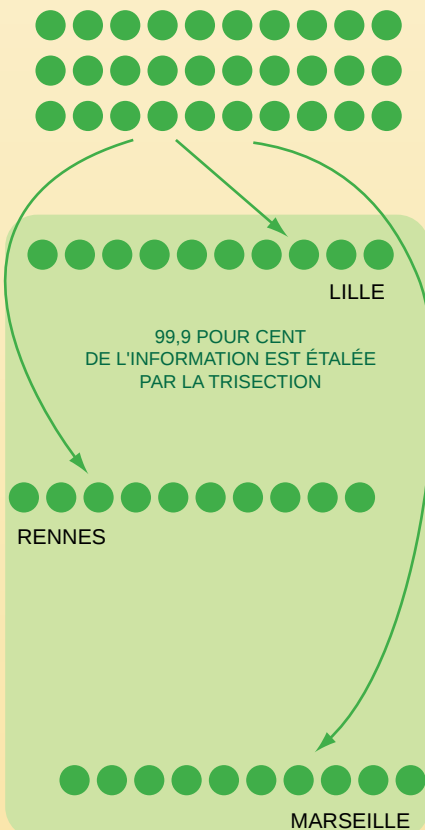
Un état général du 3-qubit est de la forme :

$$a_{000} |000\rangle + a_{001} |001\rangle + a_{010} |010\rangle + a_{011} |011\rangle + a_{100} |100\rangle + a_{101} |101\rangle + a_{110} |110\rangle + a_{111} |111\rangle,$$

où la somme des carrés des $|a_{ijk}|$ est égale à 1.

La lecture du 3-qubit donne un vecteur de la base, chaque vecteur de la base étant obtenu avec une probabilité proportionnelle à $|a_{ijk}|$.

e)



d) Réaliser un calcul quantique consiste à préparer un N-qubit dans un état initial standard, par exemple $|00\dots 0\rangle$ puis à appliquer à cet état une série de transformations unitaires (ce sont des opérations analogues en dimension quelconque aux rotations d'un vecteur). À la fin de cette suite de transformations, on mesure le N-qubit par une expérience qui l'amène dans un état correspondant à un vecteur de la base orthogonale, ce qui donne par exemple $|001\rangle$. Le résultat de cette mesure est probabiliste : on ne sait jamais ce que l'on va trouver. Tout l'art de la programmation quantique réside dans le choix des opérateurs qu'on applique de façon à ce qu'il se produise quelque chose d'intéressant (par exemple, la factorisation d'un entier). Le plus souvent, un calcul quantique commence par la création d'une superposition homogène de tous les états de la base. Pour un 3-qubit, par exemple, on commence par créer : $[|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle] / \sqrt{8}$. Un N-qubit est un objet difficile à décrire : il faut, pour le spécifier complètement, indiquer 2^N nombres complexes.

Il n'était pas évident que les règles délicates du calcul quantique par transformations unitaires produisent des résultats intéressants. C'est pourtant ce qu'ont montré Peter Shor, Lov Grover et les algorithmiciens quantiques.

e) La non-localité : un résultat de Don Page

La possibilité de coder des informations globalement dans un N-qubit est mise en évidence par l'exemple suivant : un de vos amis choisit un 30-qubit et en prépare un très grand nombre d'exemplaires (comme il l'a choisi lui-même, cela ne contredit pas le principe de non-duplication). En faisant une série assez longue de mesures sur les divers exemplaires du 30-qubit on peut en reconstituer l'état avec exactitude. Mais, au lieu de cela, on divise chaque 30-qubit en trois sous-ensembles de 10-qubit qu'on envoie à Rennes, Lille et Marseille. En faisant des mesures localement et indépendamment dans ces trois villes (c'est-à-dire sans coordonner ni corrélérer les mesures), on ne peut, d'après un résultat de Don Page, tirer en moyenne que moins d'un millième de l'information contenue dans le 30-qubit, et cela quel que soit le nombre de copies dont on dispose. L'information contenue dans le 30-qubit est intrinsèquement non locale, les composantes sont corrélées, et seules des mesures collectives peuvent la révéler.