Chapitre 16

L'information quantique, fruit de l'intrication

"Sachez, mes filles, que nous sommes des atomes
jetés dans le gouffre sans fond de l'infini."
Christophe, La famille Fenouillard

16.1 L'information quantique : comment tirer profit d'un embarras

Longtemps, le résultat de Bell engendra de nombreuses aventures expérimentales et théoriques, de nature diverse mais restreintes à de la physique fondamentale. La difficulté de ces expériences et leur sophistication croissante allaient de pair avec une multiplication de tentatives pour se défaire de l'embarras que causait l'intrication quantique, qui semblait aller de soi en pratique, mais menait à une impasse conceptuelle incroyable qui n'a pas encore trouvé d'issue. Les physiciens voulaient se défaire de leur incompréhension. La littérature sur le sujet ainsi que sur tous les concepts nouveaux et les technologies correspondantes, est plus qu'abondante[1]. Et l'intrication, elle, tenait bon : on a pu notamment vérifier que l'intrication de photons dans l'espace libre persiste à une distance de 143 km entre La Palma et Tenerife, aux îles Canaries.[2] Mais dans les années 1980, les scientifiques, physiciens, informaticiens, puis d'autres jusqu'aux médecins à l'heure actuelle, se sont aperçu que la corrélation non-locale des états quantiques intriqués pouvait, en réalité, être exploitée comme une nouvelle ressource naturelle, non-classique, plutôt qu'un ennui qu'on laissait avec respect aux amateurs éclairés ou ambitieux, et aux philosophes.

L'ensemble de ces recherches et découvertes se nomme l'information quantique. On baptise parfois cette activité foisonnante comme étant la "Seconde révolution quantique". Nous allons en décrire succinctement quelques aspects.

1. On pourra, par exemple, se référer à *Quantum Entanglement and Information*, Stanford Encyclopedia of Philosophy, Révisé en 2015 ; https ://plato.stanford.edu/entries/qt-entangle/
2. Herbst, T., Scheidl, T., Fink, M., Handsteiner, J., Wittmann, B., Ursin, R., Zeilinger, A., 2014. « Teleportation of Entanglement over 143 km », arxiv.org/abs/1403.0009.

16.2 La téléportation quantique.

Une des premières idées d'application de l'intrication quantique, réside dans une opération étonnante : la « téléportation quantique ». Puisque des états intriqués communiquent instantanément, on peut certainement concevoir une méthode de télégraphie correspondante. Cette idée a été élaborée en 1993 par C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, et W. K. Wootters[3]. Dans une paire de particules intriquées, si l'on inscrit sur l'état de l'une d'entre elles l'information que l'on souhaite communiquer, cette information sera portée immédiatement sur l'autre. Reste à savoir inscrire cette information en préservant l'intrication, et, pour le correspondant, à la déchiffrer. En pratique, Alice possède une particule A de spin $1/2$, dans l'état de spin

$$|A\rangle = \alpha|+\rangle + \beta|-\rangle \qquad \text{avec} \qquad |\alpha|^2 + |\beta|^2 = 1 \ . \tag{16.1}$$

Elle souhaite téléporter[4], c'est-à-dire « faxer », cet état à Bob de façon simple, sans avoir à mesurer elle-même α et β, et sans risquer d'être espionnée.

Le système de communication mis à la disposition d'Alice et de Bob, figure 16.1, consiste en deux parties : une liaison téléphonique habituelle, et une *source EPR*. Cette dernière, dont Alice et Bob disposent *en commun*, consiste en un émetteur d'une paire de particules B et C de spin $1/2$, l'une, B, en connexion avec Alice, l'autre, C, avec Bob. Les particules B et C sont préparées dans l'état singulet :

$$|BC\rangle = \frac{1}{\sqrt{2}}\left(|+;-\rangle - |-;+\rangle\right) \ , \tag{16.2}$$

si bien que toute information sur le spin de B sera répercutée sur celui de C.

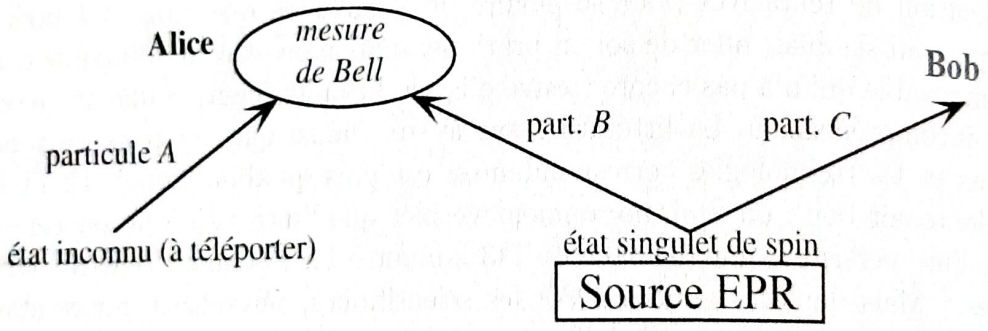

Fig. 16.1. *Principe de la téléportation de l'état quantique d'une particule.*

Alice veut "inscrire" l'état (16.1), de la particule A sur la particule B, sans détruire l'intrication de B et C. En "lisant" l'état de la particule C, Bob devra pouvoir lire et enregistrer cet état.

---

3. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, et W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. 70 1895-1899 (1993).

4. Le terme même de téléportation, qui paraissait être de la science-fiction, a été introduit par ces six physiciens.

Ici, va intervenir un mode, ou code, de communication reposant sur le système des deux particules A et B. En effet, il ne s'agit pas de faire interagir ces spins, mais, nous allons le voir, d'effectuer une mesure du spin du système AB. Afin de mener à bien l'opération, on introduit une base intéressante des états à deux spins : la base des *états de Bell*[5] (les états à deux photons se traitent de façon analogue).

États de Bell

L'état le plus général d'un système de deux spins 1/2, s'écrit :

$$\alpha|+;+\rangle + \beta|+;-\rangle + \gamma|-;+\rangle + \delta|-;-\rangle \tag{16.3}$$

avec $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. La probabilité de trouver dans une mesure $(+\hbar/2, +\hbar/2)$ est $|\alpha|^2$, celle de trouver $(+\hbar/2, -\hbar/2)$ est $|\beta|^2$, etc.

Les quatre états de la *base de Bell* sont donc définis par :

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}\left(|+;+\rangle + |-;-\rangle\right) \qquad |\Phi_+\rangle = \frac{1}{\sqrt{2}}\left(|+;-\rangle + |-;+\rangle\right)$$
$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}\left(|+;+\rangle - |-;-\rangle\right) \qquad |\Phi_-\rangle = \frac{1}{\sqrt{2}}\left(|+;-\rangle - |-;+\rangle\right) \tag{16.4}$$

Ces quatre états forment une base orthonormée du système des deux spins. On note que $|\Phi_-\rangle$ est l'état de spin total $S = 0, M = 0$ et les trois autres les combinaisons d'états $S = 1$ pour lesquels $\langle M\rangle = 0$.

Les projecteurs $P_\Psi = |\Psi\rangle\langle\Psi|$ sur chacun de ces états $|\Psi\rangle$ sont appelés opérateurs associés à *l'occupation* de cet état. En effet, les valeurs propres de ces opérateurs sont 1 (état occupé) et 0 (état non-occupé).

Un calcul direct donne les probabilités d'occupation de l'état (16.3) dans chacun des états de Bell.

état $|\Psi_+\rangle$ occupé : probabilité $|\alpha + \delta|^2/2$
état $|\Psi_-\rangle$ occupé : probabilité $|\alpha - \delta|^2/2$
état $|\Phi_+\rangle$ occupé : probabilité $|\beta + \gamma|^2/2$
état $|\Phi_-\rangle$ occupé : probabilité $|\beta - \gamma|^2/2$

La somme de ces quatre probabilités est bien égale à 1.

Téléportation

Pour qu'Alice téléporte l'état $\alpha|+\rangle + \beta|-\rangle$ de la particule A vers Bob, on convient d'une procédure. Puisque B et C de spin 1/2, sont préparées dans l'état singulet (cf. figure 16.1) : $\left(|+;-\rangle - |-;+\rangle\right)/\sqrt{2}$, le protocole de la téléportation est le suivant.

1. L'état du système formé par les *trois spins* (A, B, C) s'écrit :

$$|\Psi\rangle = \frac{\alpha}{\sqrt{2}}|+;+;-;\rangle + \frac{\beta}{\sqrt{2}}|-;+;-;\rangle - \frac{\alpha}{\sqrt{2}}|+;-;+;\rangle - \frac{\beta}{\sqrt{2}}|-;-;+;\rangle\ . \tag{16.5}$$

5. S. L. Braunstein, A. Mann, and M. Revzen, *Maximal violation of Bell inequalities for mixed states*, Phys. Rev. Lett. **68**, 3259, (1992)

Cet état se décompose sur la base de Bell du système des spins A et B, la base pour le spin C restant $|\pm\rangle$, selon :

$$|\Psi\rangle = \frac{1}{2}|\Psi_+(AB)\rangle\,(\alpha|-\rangle - \beta|+\rangle) + \frac{1}{2}|\Psi_-(AB)\rangle\,(\alpha|-\rangle + \beta|+\rangle)$$
$$- \frac{1}{2}|\Phi_+(AB)\rangle\,(\alpha|+\rangle - \beta|-\rangle) - \frac{1}{2}|\Phi_-(AB)\rangle\,(\alpha|+\rangle + \beta|-\rangle) \quad (16.6)$$

Sur lesquels on voit que les probabilités de trouver $\pm\hbar/2$ en mesurant le spin de C sont soit les mêmes que celles de trouver les mêmes valeurs pour A, soit ces valeurs interverties. Les amplitudes de probabilité peuvent être de signe différent.

Alice effectue une mesure de l'état de spin du couple de particule AB qui projette cet état sur un des quatre vecteurs de la base de Bell de AB, la probabilité de trouver la paire AB dans chacun des états de Bell est la même $(|\alpha|^2 + |\beta|^2)/4 = 1/4$. Le résultat d'Alice détermine l'état de C, mesuré pas Bob.

Le principe de la mesure de l'état de Bell est simple si l'on opère avec des photons polarisés, ce qui est le cas en pratique. Cela revient à un jeu de lames biréfringentes [6].

2. Si Alice trouve la paire AB dans l'état $|\Phi_-(AB)\rangle$, l'état du spin C est l'état de départ $\alpha|+\rangle + \beta|-\rangle$. Si Alice trouve cette paire dans l'un des trois autres états : $|\Psi_+(AB)\rangle$, $|\Psi_-(AB)\rangle$ ou $|\Phi_+(AB)\rangle$, les composantes α et β se déduisent de l'état de C par des changements de signe correspondant à des transformations simples.

3. Pour téléporter l'état *a priori* inconnu $\alpha|+\rangle + \beta|-\rangle$ de la particule A vers la particule C, Alice ne doit pas chercher à mesurer cet état. Elle doit « simplement » effectuer une mesure de l'état de Bell de la paire AB et *communiquer classiquement* (téléphoner) le résultat à Bob. Si elle trouve que c'est l'état $|\Phi_-\rangle$ qui est occupé (dans 25% des cas), Bob n'a rien à faire : il lit ou utilise l'état du spin C qui est égal à l'état du spin A avant mesure de Bell.

   Dans trois les autres cas, Bob, après avoir capté l'état de C, peut reconstruire l'état initial au moyen d'une transformation simple. Par exemple, si Alice trouve la paire AB dans l'état de Bell $|\Phi_+\rangle$, l'état du spin C est $\alpha|+\rangle - \beta|-\rangle$, qui peut se ramener à l'état initial $\alpha|+\rangle + \beta|-\rangle$ en effectuant une rotation d'un angle π autour de z.

   En notations quantiques, Bob retrouve l'état A dans ces trois cas en appliquant à l'état de C les matrices de Pauli : $\hat{\sigma}_z$ dans le cas $|\Phi_+\rangle$, $\hat{\sigma}_x$ dans le cas $|\Psi_-\rangle$ et $-i\hat{\sigma}_y$ dans le cas $|\Psi_+\rangle$. Cela correspond à l'application de portes logiques en informatique.

---

6. Yoon-Ho Kim, Sergei P. Kulik, and Yanhua Shih, *Quantum Teleportation of a Polarization State with a Complete Bell State Measurement*, Phys. Rev. Lett. **86**, 1370, (2001)

4. Tout cela se visualise très simplement en revenant à des états de photons. Les états de Bell sont alors :

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|\rightarrow;\uparrow\rangle + |\uparrow;\uparrow\rangle) \qquad |\Phi_+\rangle = \frac{1}{\sqrt{2}}(|\rightarrow;\uparrow\rangle + |\uparrow;\rightarrow\rangle)$$
$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|\rightarrow;\rightarrow\rangle - |\uparrow;\uparrow\rangle) \qquad |\Phi_-\rangle = \frac{1}{\sqrt{2}}(|\rightarrow;\uparrow\rangle - |\uparrow;\rightarrow\rangle) \quad (16.7)$$

Si l'état (de polarisation linéaire, donc α et β réels) est $|A\rangle = \alpha|\rightarrow\rangle + \beta|\uparrow\rangle$ et l'état intriqué $|BC\rangle = (|\rightarrow,\uparrow\rangle - |\uparrow,\rightarrow\rangle)/\sqrt{2}$. On voit que la mesure des états de Bell $|\Phi_+(AB)\rangle$, $|\Psi_-(AB)\rangle$, et $|\Psi_+(AB)\rangle$ donnent lieu à des symétries simples par rapport à la verticale ou à la première diagonale.

5. En raison du théorème de non clonage, que nous verrons à propos de la cryptographie, la transmission du message quantique d'Alice à Bob est complètement sécurisée.

6. On ne peut évidemment pas utiliser ce principe pour transmettre de l'information plus vite que par des voies classiques. Tant qu'Alice n'a pas indiqué à Bob le résultat de sa mesure de Bell, Bob ne dispose d'aucune information valable. C'est uniquement quand il a pris connaissance du résultat d'Alice, et qu'il a identifié les transformations simples à faire sur l'état de C, qu'il peut tirer parti de cette « téléportation » et reconstruire de l'état quantique de la particule A.

7. Le seul intervalle de temps non nul dans cette opération est la transmission de l'information classique d'Alice à Bob sur lequel des 4 états de Bell est à considérer, ce qui déterminera l'état de C, comme on le voit sur (16.6).

8. Un exemple d'application frappant est le suivant. Alice veut transmettre à Bob la direction dans l'espace de la polarisation d'un photon. Par le transport quantique, Bob reconstitue *exactement* le photon d'Alice et la direction de sa polarisation. Pour le faire de façon classique, étant donné que la polarisation, vecteur de l'espace, est définie par ses coordonnées, on ne peut espérer que fixer une limite à la marge d'erreurs et procéder par des ajustements successifs.

   Imaginons qu'un tel procédé soit appliqué en matière de détection radar : dans une paire intriquée, un photon envoyé dans une certaine direction atteint un objet. Supposons que son état de polarisation soit modifié de façon identifiable dans cette interaction, cette modification serait transmise instantanément à son partenaire intriqué, demeuré (si l'on peut dire) dans l'émetteur. Cela permettrait de distinguer le signal du bruit de fond avec un contraste inimaginable. Il reste à définir et à mettre au point des protocoles pratiques pour rendre l'exploration de cette voie opérationnelle.

9. *L'échange d'intrication* découle assez directement de ce que nous de venons voir. Considérons deux sources EPR de photons, AB et CD, éloignées d'une certaine distance. Les photons A et B, émis par la source AB sont dans l'état $|\Phi_-\rangle_{AB}$, et les photons C et D dans l'état $|\Phi_-\rangle_{CD}$. L'état du système global est

$$|\Psi\rangle_{ABCD} = |\Phi_-\rangle_{AB}|\Phi_-\rangle_{CD}\,.$$

Les photons B et C sont transmis à une station centrale où l'on effectue une mesure de Bell du système BC, alors que les photons A et D se dirigent vers d'autres directions, plus éloignées. Un exercice simple montre que l'état $|\Psi\rangle_{ABCD}$ se décompose sur la base de Bell de BC selon :

$$|\Psi\rangle_{ABCD} = \frac{1}{2}(|\Psi_+\rangle_{AD}|\Psi_+\rangle_{BC} - |\Psi_-\rangle_{AD}|\Psi_-\rangle_{BC} - |\Phi_+\rangle_{AD}|\Phi_+\rangle_{BC} + |\Phi_-\rangle_{AD}|\Phi_-\rangle_{BC}) . \tag{16.8}$$

Par conséquent, une mesure de Bell sur les photons B et C, produit une intrication des photons A et D. Comme dans la téléportation, il faut transmettre par voie classique à A et D le résultat de la mesure de Bell sur BC, à la suite de quoi ils pourront effectuer la transformation décrite plus haut. Une application évidente est de pouvoir ainsi augmenter la distance des sources EPR. On peut en imaginer d'autres.

Résultats expérimentaux et généralisations

La première mise en oeuvre expérimentale de cette technique est due à A. Zeilinger et ses collaborateurs [7]. Un compte rendu très complet, théorique et expérimental, de la téléportation quantique se trouve dans les publications de Nicolas Gisin [8].

La généralisation à un grand nombre de photons, ou à des ondes électromagnétiques cohérentes, encore appelée « téléportation quantique en variables continues » a été faite à Caltech par Kimble et ses collaborateurs en 1998 [9], à l'aide d'états comprimés de photons. La description de cette technique, largement utilisée en pratique, requiert des notions de quantification du champ électromagnétique que nous ne traitons pas ici (elle procède de la même idée). On étudie également des systèmes de réseaux de communications quantiques [10]. L'idée de départ est de former un système de téléportation à trois faisceaux intriqués, en utilisant comme source EPR les état intriqués de trois photons GHZ dont nous avons parlé au chapitre 15, §15.5.

Un record actuel de transmission quantique est celui de chercheurs de Calgary [11], dans l'Alberta, qui sont parvenus à faire fonctionner, dans cette ville, un réseau de téléportation par fibres optiques dans un rayon de 6 km.

---

7. Dik Bouwmeester , Jian-Wei Pan , Klaus Mattle, Manfred Eibl, Harald Weinfurter, Anton Zeilinger, *Experimental quantum teleportation* Nature **390**, 575, (1997) ; Phil. Trans. R. Soc. Lond. A **356**, 1733, (1998)

8. N. Gisin et al., *Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory*, Nature Photonics **8**, 775, (2014) ; *Téléportation quantique*, http ://dpnc.unige.ch/conferences/gisin.pdf

9. A. Furusawa, J. L. Sörensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik *Unconditional Quantum Teleportation*, Science, **282**, Issue 5389, 706, 1998.

10. H. Yonezawa, T. Aoki, and A. Furusawa, *Demonstration of a quantum teleportation network for continuous variables*, Nature **431**, (2004)

11. Raju Valivarthi, Marcel.li Grimau Puigibert, et **al**, *Quantum teleportation across a metropolitan fibre network*, Nature Photonics **10**, 676 (2016)

Le record absolu de distance, vivement relayé par la presse internationale, est celui de chercheurs chinois [12]. Depuis 2003 et avec la progression économique que l'on sait, la Chine connaît un essor considérable dans la recherche et le développement de technologies de pointe. Jian-Wei Pan à l'Université de Sciences et Technologie de Chine (USTC) à Shanghai, qui a effectué son travail de thèse avec A. Zeilinger à Innsbrück, et coopère avec ce dernier, a créé un groupe sur le plan de recherche QUESS ("Quantum Experiments at Space Scale", Expériences quantiques à l'échelle spatiale). Ces recherches ont effectué plusieurs percées dans le domaine de la téléportation quantique qui ont permis de créer de nouvelles perspectives pour les télécommunications quantiques à longue distance. Les chercheurs ont utilisé le satellite scientifique *Mozi* (nom d'un célèbre philosophe chinois) lancé en août 2016 depuis la base de Jiuquan, dans le désert de Gobi, sur une orbite héliosynchrone dont l'apogée est de 584 km et le périgée de 488 km. Puis, ils ont réalisé une téléportation quantique du sol depuis l'espace.

En 2017, ce satellite a permis de faire faire un bond au record de portée de l'intrication quantique, le portant à 1203 km en effectuant la transmission d'une paire de photons intriqués vers les stations terrestres de Delingha, sur le plateau tibétain, et l'observatoire Gaomeigu à Lijiang, au nord du Yunnan.

Outre la preuve du maintien de l'intrication sur de telles distances, les perspectives sont d'abord de transmettre une clé quantique entre Pékin et Vienne, puis, à terme, la Chine envisage de lancer trente satellites de communication quantique d'ici 2030 pour couvrir l'ensemble de la Terre. Il y a évidemment de sérieux problèmes pratiques à résoudre comme de bien pointer les récepteurs au sol sur le satellite aux distances envisagées. L'avantage de l'espace dans ces projets est qu'il perturbe beaucoup moins les signaux que l'atmosphère.

La télécommunication quantique permettrait notamment, si le projet d'ordinateur quantique prend réellement forme, de connecter des milliers de calcul différents à un même ordinateur quantique central, dont la vitesse sera considérable, nous le verrons, mais dont la construction et l'entretien seraient d'une complexité et d'un prix exorbitants si l'on envisageait d'en construire de grandes quantités.

16.3 La cryptographie quantique

Le but de la cryptographie est la transmission d'un message d'un émetteur (Alice) vers un récepteur (Bob), en minimisant les risques qu'un espion puisse intercepter et décoder ce message. La cryptographie classique fait pour cela appel à des méthodes de codage sophistiquées (comme la factorisation d'un nombre très grand, construit comme le produit de deux autres nombres premiers), qui ne peuvent pas être « cassées » en un temps raisonnable compte tenu des moyens de calcul actuellement disponibles. La cryptographie quantique fonctionne sur un principe différent : elle permet à Alice et Bob de s'assurer qu'aucun espion n'a intercepté le message échangé !

12. Ji-Gang Ren, Ping Xu, Jian-Wei Pan et **al.**, *Ground-to-satellite quantum teleportation*, Nature **549**, 70 (2017) ; Juan Yin, Yuan Cao, Jian-Wei Pan et **al.**, *Satellite-based entanglement distribution over 1200 kilometers*, Science, **356**, Issue 6343, 1140 (2017)

Le principe de cette technique est de tirer parti du fait qu'en mécanique quantique *une mesure perturbe l'état du système* notamment sur les états intriqués. On met donc sur pied un protocole qui dévoilera la présence éventuelle d'un espion *avant* d'envoyer le contenu du message !

La communication entre Alice et Bob

Un message peut toujours être codé en langage binaire, c'est-à-dire par une suite de 0 et de 1. Chaque nombre, 0 ou 1, représente une information élémentaire, ou encore un *bit*. Pour transmettre son message, nous supposerons qu'Alice envoie vers Bob un faisceau de particules de spin 1/2, avec un flux bien contrôlé, et que Bob mesure une composante du spin de chacune de ces particules. Chaque particule transporte par l'intermédiaire de son état de spin un bit. On peut convenir que $+\hbar/2$ est 1 et $-\hbar/2$ est 0.

Supposons dans un premier temps qu'Alice envoie chaque particule dans l'état $|+z\rangle$ ou $|-z\rangle$. Par convention $|+z\rangle$ représente la valeur 1 et $|-z\rangle$ la valeur 0. Bob oriente son appareil le long de l'axe z, mesure l'état de spin des particules qui arrivent et reconstitue ainsi le message d'Alice. Une telle procédure n'a rien de spécifiquement quantique et peut facilement être espionnée. Il suffit que l'espion, situé entre Alice et Bob, dispose lui-même d'un appareil qu'il oriente également selon l'axe z. Il mesure l'état de spin de chaque particule incidente suivant cet axe, puis émet vers Bob une particule avec un état de spin identique. Il prend ainsi connaissance du message sans qu'Alice et Bob ne puissent détecter sa présence.

La situation change radicalement si Alice choisit, pour chacune des particules qu'elle envoie, un des quatre états $|+z\rangle$, $|-z\rangle$, $|+x\rangle$ ou $|-x\rangle$, sans indiquer à quiconque l'axe choisi (x ou z) pour une particule donnée. Supposons qu'Alice envoie vers Bob une série de particules sans chercher pour l'instant à former un message intelligible. Ces particules sont au nombre de 16 sur les figures 16.2, et 16.3, mais sont beaucoup plus nombreuses en pratique. Ce n'est qu'à la fin de la procédure qu'Alice décidera quelles sont les particules à prendre en compte pour construire le message qu'elle souhaite transmettre.

Bob procède de la manière suivante. Il oriente de manière aléatoire l'axe de son appareil suivant x ou z. Pour la moitié des particules (en moyenne), son choix coïncide avec celui d'Alice. Dans ce cas, le bit qu'il détecte est significatif : si Alice a envoyé une particule $|+x\rangle$ et si Bob oriente son appareil selon la direction x, il mesure effectivement $+$ avec une probabilité de 1. Pour l'autre moitié des particules, Bob ne choisit pas le même axe qu'Alice et sa mesure est sans intérêt : si Alice a envoyé $|+x\rangle$ et si Bob choisit l'axe z, alors il détecte $+$ avec une probabilité $1/2$ et $-$ avec une probabilité $1/2$.

Pour s'assurer qu'un espion n'a pas intercepté la transmission, Bob diffuse publiquement l'ensemble de ses choix d'axes, x ou z, ainsi qu'une fraction des résultats obtenus, $+$ ou $-$. Par exemple, pour les 16 particules des figures 16.2 et 16.3, Bob diffuse publiquement ses 16 choix d'axes, ainsi que les 8 premiers résultats obtenus. À l'examen de ces résultats, Alice peut détecter la présence éventuelle d'un espion. Son raisonnement est le suivant. L'espion ne connaît pas plus que Bob l'orientation x ou z qu'elle a choisie pour chaque particule. Supposons donc que l'espion oriente lui aussi son appareil de manière arbitraire selon x ou z, et qu'il émette à chaque détection une

Numéro de la particule	1	2	3	4	5	6	7	8
Axe choisi par Alice (gardé secret)	z	z	x	z	z	x	x	z
état choisi par Alice (gardé secret)	+	−	+	−	−	−	+	−
Axe choisi par Bob (diffusé publiquement)	z	x	x	z	x	z	x	x
état mesuré par Bob (diffusé publiquement)	+	−	+	−	−	+	+	+
Mesure utile ?	oui	non	oui	oui	non	non	oui	non

Fig. 16.2. *Détection éventuelle d'une espion : Alice recherche parmi les mesures effectuées avec le même choix d'axes par Bob et par elle-même (particules 1,3,4 et 7) une éventuelle différence dans les états, qui signalerait la présence d'un espion. Aucune anomalie ne se produit ici. Pour s'assurer de l'absence d'un espion avec une probabilité raisonnable, il faut utiliser en pratique un nombre de mesures bien supérieur à 8.*

particule dont l'état de spin est identique à ce qu'il vient de mesurer. Ainsi, s'il choisit l'axe x et qu'il mesure +, il émet vers Bob une particule $|+x\rangle$. Un tel comportement est en fait détectable car il introduit des erreurs au niveau des détections de Bob.

Considérons par exemple le cas où Alice a envoyé une particule $|+z\rangle$, où Bob a également orienté son appareil selon l'axe z, mais où l'espion a orienté son appareil selon x. L'espion va mesurer + avec une probabilité $1/2$ et − avec une probabilité $1/2$. Selon son résultat, il émet ensuite vers Bob une particule dans l'état $|+x\rangle$ ou $|-x\rangle$. Dans les deux cas, avec son appareil de Stern et Gerlach orienté selon z, Bob peut mesurer + avec une probabilité $1/2$ et − avec une probabilité $1/2$. Si l'espion n'avait pas été présent, Bob aurait dû mesurer + avec une probabilité de 1.

Alice va donc s'intéresser, parmi tous les résultats diffusés publiquement par Bob, à ceux où son propre choix d'axes coïncide avec celui de Bob (figure 16.2). Si aucun espion n'est présent, les résultats de Bob doivent être identiques à ce qu'a émis Alice. Dans le cas contraire, il doit y avoir des différences dans 25% des cas. Ainsi, si Bob annonce publiquement 1000 résultats, 500 en moyenne seront utilisables par Alice, et un espion aura introduit une erreur pour 125 d'entre eux, toujours en moyenne. La probabilité pour qu'un espion effectivement présent ne soit pas détecté par une telle procédure est de $(3/4)^{500} \sim 3 \times 10^{-63}$, ce qui est négligeable.

Une fois qu'Alice s'est assurée qu'aucun espion n'a intercepté leur communication, elle diffuse publiquement le numéro des mesures que Bob doit considérer pour reconstruire le message qu'elle souhaite transmettre. Elle les choisit simplement parmi la suite de bits pour lesquels Bob et elle ont fait le même choix d'axes, et pour lesquels Bob n'a pas diffusé publiquement son résultat (*cf* figure 16.3).

Le théorème de non-clonage quantique

Dans le paragraphe qui précède, nous avons supposé que l'espion choisissait de manière arbitraire l'orientation de son appareil pour chaque particule, puis émettait vers Bob une particule dans un état de spin correspondant à son résultat de mesure. On peut se demander s'il s'agit de la meilleure stratégie pour lui éviter d'être détecté.

Numéro de la particule	9	10	11	12	13	14	15	16
Axe choisi par Alice (gardé secret)	x	z	x	z	z	x	z	z
état choisi par Alice (gardé secret)	+	−	+	+	−	−	+	−
Axe choisi par Bob (diffusé publiquement)	z	z	x	x	z	z	z	x
état mesuré par Bob (gardé secret)	−	−	+	+	−	+	+	+
Mesure utile ?	non	oui	oui	non	oui	non	oui	non

Fig. 16.3. *Après s'être assurée de l'absence d'un espion, Alice choisit parmi les mesures utiles celles qui lui permettent de communiquer son message. Par exemple, pour communiquer le message « 1,1 » , c'est-à-dire « +, + » , elle demande (publiquement) à Bob de considérer les résultats de ses mesures 11 et 15.*

En particulier, si l'espion pouvait cloner la particule incidente émise par Alice en deux autres particules avec le même état de spin, il lui serait possible de renvoyer vers Bob une de ces deux particules, tout en gardant l'autre particule pour effectuer sa propre mesure. L'espion serait alors indétectable.

Ce clonage d'un état inconnu est (heureusement pour Alice et Bob) impossible en mécanique quantique [13]. On ne peut pas générer de manière fiable une ou plusieurs copies d'un état quantique, à moins que cet état ne soit partiellement connu auparavant. Pour démontrer ce résultat, notons $|\alpha_1\rangle$ un état quantique original à dupliquer. Le système sur lequel la copie doit « s'imprimer » est initialement dans un état connu que nous notons $|\phi\rangle$ (l'équivalent d'une feuille blanche dans une photocopieuse). L'évolution du système total *original + copie* durant l'opération de clonage doit donc être :

$$\text{clonage :} \qquad |\text{original} : \alpha_1\rangle|\text{copie} : \phi\rangle \longrightarrow |\text{original} : \alpha_1\rangle|\text{copie} : \alpha_1\rangle \tag{16.9}$$

Cette évolution est régie par un hamiltonien que nous ne chercherons pas à préciser, mais qui ne dépend pas de $|\alpha_1\rangle$ puisque celui-ci est par hypothèse inconnu. Pour un autre état de l'original $|\alpha_2\rangle$ (orthogonal à $|\alpha_1\rangle$), on doit également avoir :

$$\text{clonage :} \qquad |\text{original} : \alpha_2\rangle|\text{copie} : \phi\rangle \longrightarrow |\text{original} : \alpha_2\rangle|\text{copie} : \alpha_2\rangle \ . \tag{16.10}$$

L'impossibilité du clonage apparaît alors pour l'état initial

$$|\alpha_3\rangle = \frac{1}{\sqrt{2}}\left(|\alpha_1\rangle + |\alpha_2\rangle\right) \ . \tag{16.11}$$

Si l'opération de copie fonctionne pour cet état, on doit trouver :

$$\text{clonage :} \qquad |\text{original} : \alpha_3\rangle|\text{copie} : \phi\rangle \longrightarrow |\text{original} : \alpha_3\rangle|\text{copie} : \alpha_3\rangle \ . \tag{16.12}$$

Mais la linéarité de l'équation de Schrödinger impose par combinaison linéaire de (16.9) et (16.10) :

13. W. K. Wooters et W. H. Zurek, Nature **299**, 802 (1982).

$$|\text{original} : \alpha_3\rangle|\text{copie} : \phi\rangle \longrightarrow$$
$$\frac{1}{\sqrt{2}}\left(|\text{original} : \alpha_1\rangle|\text{copie} : \alpha_1\rangle + |\text{original} : \alpha_2\rangle|\text{copie} : \alpha_2\rangle\right) .$$

Cet état final intriqué est différent de l'état souhaité (16.12).

L'examen de cette démonstration permet de comprendre l'apport de la mécanique quantique à la cryptographie. Si on se limite à une transmission à deux états $|\alpha_1\rangle = |+ z\rangle$ et $|\alpha_2\rangle = |- z\rangle$, alors l'espion peut rester indétectable comme nous l'avons vu au début du paragraphe précédent. Les deux opérations (16.9) et (16.10) sont possibles, ne serait-ce qu'en mesurant l'état de spin de la particule incidente le long de l'axe z, puis en émettant une (ou plusieurs) particules dans le même état. C'est le fait de pouvoir utiliser simultanément les états $|\alpha_1\rangle$, $|\alpha_2\rangle$ et des combinaisons linéaires de ces états $|\alpha_3\rangle = |\pm : x\rangle$ qui fait l'originalité de la cryptographie quantique, et qui interdit toute duplication fiable d'un message intercepté par un espion.

Les montages expérimentaux

Comme pour les tests de l'inégalité de Bell ou dans la téléportation quantique, les montages réels utilisent des photons plutôt que des particules de spin 1/2. Diverses méthodes peuvent être utilisées pour coder l'information sur les photons ; nous considérerons seulement le codage en polarisation, qui est effectivement utilisé en pratique. Alice utilise quatre états définissant deux bases non orthogonales, qui permettent chacune de coder les bits 0 et 1, par exemple sous la forme :

$$|\uparrow\rangle : 1 \qquad |\rightarrow\rangle : 0 \qquad |\nearrow\rangle : 1 \qquad |\nwarrow\rangle : 0 \tag{16.13}$$

Un enjeu des montages réels de cryptographie quantique est d'obtenir une distance de ransmission suffisante. On obtient actuellement des distances de l'ordre de quelques izaines de kilomètres, en utilisant des techniques empruntées aux télécommunications optiques, et en particulier en transmettant les photons dans des fibres optiques.

Un point important à considérer est la source lumineuse utilisée. Le théorème e non clonage quantique, essentiel pour garantir la sécurité du système, s'applique à des photons considérés individuellement. Au contraire, les impulsions lumineuses généralement utilisées dans les systèmes de télécommunications contiennent un très grand nombre de photons, typiquement plus de 10^6. Si l'on utilise un codage en polarisation pour de telles impulsions, le théorème de non clonage quantique ne s'applique pas. L'espion peut prélever pour chaque impulsion une petite partie de la lumière envoyée par Alice, et il peut ainsi identifier la polarisation utilisée, en introduisant des erreurs négligeables dans la transmission. Pour garantir la sécurité du message, il faut donc en principe que chaque impulsion contienne un photon et un seul. Cette condition est difficile à obtenir, et on se contente en pratique de la méthode suivante : Alice atténue fortement les impulsions pour que la probabilité p d'avoir un photon dans chaque impulsion soit petite devant un. La probabilité d'avoir deux photons sera alors $p^2 \ll p$, ce qui signifie que les impulsions à deux photons (ou davantage) seront très peu nombreuses. évidemment, la plupart des impulsions ne contiendront aucun photon, ce qui est un défaut de la méthode : on doit coder l'information de manière

redondante. On considère généralement qu'une valeur de p comprise entre 0,01 et 0,1 constitue un compromis acceptable.

Cette question étant résolue, l'essentiel du montage fait appel aux technologies des télécommunications optiques. La source est un laser impulsionnel fortement atténué, et le codage en polarisation s'effectue directement dans la fibre optique grâce à des modulateurs intégrés. Les impulsions atténuées sont détectées grâce à des *photodiodes à avalanche*, qui transforment un photon unique en une impulsion électrique macroscopique grâce à un processus de multiplication d'électrons. Afin d'identifier sans ambiguïté les photons émis par Alice et détectés par Bob, des impulsions électriques synchrones du laser émetteur sont transmises par voie conventionnelle, et jouent un rôle d'horloge. Finalement, une gestion informatique est indispensable pour réaliser toutes les procédures décrites dans le paragraphe précédent, et en particulier pour tester l'absence d'espionnage sur la ligne.

Applications

À l'heure actuelle, les systèmes connus qui ont été réalisés sont davantage des prototypes de démonstration plutôt que des systèmes opérationnels. Ils ont permis de tester divers paramètres pertinents, comme la distance et le taux de transmission, les taux d'erreurs... En fait, le développement de ces systèmes a pour l'instant un caractère prospectif, car les systèmes cryptographiques conventionnels (non quantiques) sont considérés comme très sûrs par leurs utilisateurs, civils ou militaires. Pourtant, cette confiance a été un peu ébranlée en 1994, comme nous le verrons dans le paragraphe suivant, consacré à l'ordinateur quantique.

Les progrès se font à des vitesses vertigineuses. Le premier prototype expérimental, fait en 1991 par Bennet et Brassard, portait sur une distance de 32 centimètres. En 2003, une équipe viennoise réussit une transmission intriquée entre les rives du Danube, à 500 mètres de distance. Un an plus tard, un réseau fonctionnait à Cambridge, Massachusetts, depuis MIT jusqu'à Harvard, sur des distances de 10 kilomètres. Le projet avait été financé par le Pentagone.

Il existe des applications universitaires intéressantes, comme le réseau de Cambridge : *Cambridge launches UK's first quantum network* installé en juin 2018[14].

Les applications militaires, que ce soit dans l'obtention et dans la transmission de l'information ou dans la sûreté des installations ne sont évidemment pas divulguées. On peut deviner que les succès des physiciens chinois dans la téléportation par satellites ont des répercussions considérables. Parmi tant d'autres choses, on lit, par exemple, dans des revues à grande diffusion l'effort mené par certains pays, la Chine, la Russie, le Canada, dans le développement de radars quantiques pour la détection d'avions furtifs[15]. Le Canada consacrerait 2,7 millions de dollars à ces recherches.

---

14. https ://www.cam.ac.uk/research/news/cambridge-launches-uks-first-quantum-network

15. *Canada developing quantum radar to detect stealth aircraft*, BBC News, 2017, https ://www.bbc.com/news/technology-43877682 ; *Quantum radar will expose stealth aircraft*, Christine Bezruki, Institute for Quantum Computing, University of Waterloo, 2018, https ://uwaterloo.ca/stories/ ; *Could ghost imaging spy satellite be a game changer for Chinese military ?*, China Science, Novembre 2017 https ://www.scmp.com/news/china/society/article/2121479

Dans le même ordre d'idées, on parle beaucoup également des applications dans les domaines "sensibles" : défense, police, renseignement, communications diplomatiques, constitution de dossiers cryptés inviolables sur des questions délicates.

Un domaine d'application extrêmement développé est celui du secteur financier et bancaire. À l'heure actuelle, le codage de produits courants, comme les cartes bancaires, est effectué avec des méthodes classiques éprouvées. Toutefois, tant ces informations du grand public, que les informations de plus grande ampleur, subissent de véritables et salutaires bouleversements grâce aux méthodes de cryptographie et de télécommunication quantiques. Le pourtour du Lac de Genève a été le berceau des premières installations bancaires de cryptographie quantique sur plusieurs dizaines de kilomètres. Les liaisons entre grandes villes suisses, comme Genève, Lausanne, Zurich, Bâle, sont totalement assurées (c'est souvent la question du stockage des données qui pose problème). On sait que l'océan Pacifique est une région du monde au dessus de laquelle transitent des informations financières de toute première importance. Tant la sécurité que la rapidité sont primordiales.

Pour revenir à des questions plus quotidiennes, de gros efforts de développement sont en cours dans le domaine de la santé : les dossiers individuels, le suivi, tout en gardant une confidentialité totale pour la protection des patients.

Une question importante à l'heure actuelle est de sécuriser le vote politique. La Suisse emploie ces moyens depuis 2007. De nombreux pays déclarent vouloir s'équiper de tels système sécurisés, la phase la plus vulnérable se trouvant dans le transfert des résultats.

La communication spatiale gagnera énormément avec la mise en place de modes de transmission sécurisés et rapides. La sécurité des astronautes ainsi que la bonne marche des dispositifs en orbite y trouveront des progrès appréciables.

Enfin se pose à l'heure actuelle la question cruciale de la sécurisation de la communication par Internet, et des réseaux sociaux.

16.4 L'ordinateur quantique

L'ordinateur quantique provient d'une idée encore plus fascinante[16] provenant des états quantiques[17]. Un ordinateur habituel fonctionne essentiellement de façon séquentielle, une information passant d'un mot à un autre d'un registre. Supposons, maintenant que l'on opère avec une mémoire quantique formée d'un nombre macroscopique, donc énorme, d'éléments quantiques intriqués, et que l'on laisse le système évoluer. Chaque opération élémentaire est banale, mais le nombre d'opération qui peuvent être faites *simultanément* est gigantesque. La construction (éventuelle) de grands calculateurs quantiques permettrait selon David Deutsch[18] de faire des calculs plus vite qu'un ordinateur classique plus grand que l'univers observable lui-même. Si l'on parvient à résoudre tous les problèmes pratiques en jeu, notamment l'interaction de ce système intriqué macroscopique avec le milieu extérieur, une machine

16. Richard P. Feynman, *Simulating Physics with Computers*, International Journal of Theoretical ... **21**, Nos. 6/7, 1982

17. ...n trouvera un exposé très complet dans : Michael A. Nielsen, Isaac L. Chuang, *Quantum ...putation and Quantum Information*, Cambridge University Press, 2000

18. D. Deutsch, *The Fabric of Reality*, Penguin, New Ed edition, 1998

quantique pourrait ne mettre qu'une seconde à calculer ce qui prendrait 10 000 ans à un ordinateur conventionnel. Reste aussi à savoir comment fabriquer et manipuler de tels dispositifs, et comment effectuer la lecture des résultats puisque ce processus, classique, est par nature destructif.

Les bits quantiques, ou « q-bits »

Nous avons vu dans le paragraphe précédent qu'il est possible de coder un bit d'information (0 ou 1) sur deux états orthogonaux d'une particule de spin 1/2 ou d'un photon polarisé. Que se passe-t-il alors, du point de vue du contenu d'information, si la particule est placée dans une combinaison linéaire de ces deux états ? En termes imagés, le bit ne vaudra plus 0 ou 1, mais sera dans une *superposition linéaire* de ces deux valeurs. Pour prendre en compte cette possibilité, on introduit la notion de « q-bit », ou bit quantique, qui contrairement au bit classique, admet l'existence de tels états intermédiaires. La notion de q-bit n'est en elle-même pas très riche, mais nous allons voir qu'elle a des implications intéressantes si l'on considère un ordinateur quantique, basé sur la manipulation d'un grand nombre de q-bits.

Nous prendrons une définition très simplifiée d'un ordinateur, en le considérant comme un appareil capable d'effectuer des opérations sur des ensembles de N bits appelés « registres ». Le contenu d'un registre est un mot binaire, qui représente un nombre mémorisé par l'ordinateur. Pour $N = 3$, on a ainsi 8 mots possibles :

$$(+,+,+)\,(+,+,-)\,(+,-,+)\,(+,-,-)\,(-,+,+)\,(-,+,-)\,(-,-,+)\,(-,-,-)$$

Considérons maintenant un q-registre, formé d'un ensemble de N q-bits. Les 2^N états possibles du registre classique vont alors définir une base de l'espace des états du q-registre, qui pourra quant à lui être placé dans une superposition linéaire arbitraire de tous les états de base :

$$|\Psi\rangle = \sum_{\sigma_1=\pm} \sum_{\sigma_2=\pm} \sum_{\sigma_3=\pm} C_{\sigma_1,\sigma_2,\sigma_3}\,|\sigma_1,\sigma_2,\sigma_3\rangle \qquad \text{pour } N=3\ .$$

Supposons maintenant que l'ordinateur calcule, c'est à dire effectue une opération sur l'état du q-registre. Puisque cette opération est réalisée sur une superposition linéaire d'états, on peut considérer qu'elle est effectuée « en parallèle » sur les 2^N nombres classiques. Cette notion de parallélisme quantique est à la base du gain d'efficacité de l'ordinateur, qui peut en principe être exponentiel si les 2^N calculs correspondant à N q-bits sont effectivement réalisés simultanément. (Pour fixer les idées et se repérer, avec 40 q-bits, ce qui semble peu, on atteindrait 2^{40} ~mille milliards). En fait, puisqu'il s'agit de superpositions linéaires, un q-bit peut valoir à la fois 0 et 1 en même temps, c'est-à-dire une *infinité* de valeurs comprises entre 0 et 1 (et telles que la normalisation de l'état reste normé à un). Il faut modérer cette augmentation gigantesque de capacité avec le fait qu'une seule mesure ne suffit pas puisqu'elle donne un résultat probabiliste, comme nous allons le voir ci-dessous.

De nombreuses questions se posent immédiatement : sur le plan fondamental, quel type de calculs et quel type d'algorithmes peut-on effectuer avec un tel dispositif, sur le plan pratique, comment peut-on envisager de le réaliser ?

L'algorithme de Peter Shor

Dans le paragraphe précédent, nous avons fait allusion aux systèmes cryptographiques non quantiques, qui sont souvent appelés protocoles algorithmiques. Un de ces protocoles est fondé sur le fait que certaines opérations mathématiques sont très faciles à réaliser dans un sens, mais beaucoup plus difficiles à réaliser dans l'autre. Par exemple, il est simple et rapide pour un ordinateur de calculer le produit de deux nombres ; en revanche, il est en général beaucoup plus difficile de décomposer un produit en ses facteurs premiers. Ainsi, si l'on considère le produit P de deux grands nombres premiers, il faut effectuer approximativement $\sqrt{P}$ divisions pour identifier les facteurs. Le temps de calcul augmente exponentiellement avec le nombre de chiffres (ou de bits) de P, et devient rapidement rédhibitoire. La méthode cryptographique fondée sur cette remarque et initialement proposé par Rivest, Shamir et Adelman, est actuellement très répandue (cartes bancaires, transactions électroniques...), et elle est considérée comme étant extrêmement sûre.

Aussi peut-on imaginer sans peine l'impact qu'a eu un article publié en 1994 par un chercheur américain, Peter Shor [19], qui montrait qu'un ordinateur quantique pourrait factoriser le produit de deux nombres premiers en un temps réduit d'un facteur exponentiel par rapport aux ordinateurs classiques ! L'effervescence étant maintenant retombée, la situation semble être la suivante : l'algorithme proposé par Peter Shor est correct dans son principe, et apporte bien le gain d'efficacité escompté. En revanche, la réalisation d'un ordinateur quantique compétitif semble hors de portée de la technologie actuelle, bien qu'elle ne soit pas exclue par les lois de la physique. Précisons ici qu'il apparaît dans cette situation une différence considérable entre un "calculateur" et un "ordinateur". Le premier consiste en un algorithme effectuant un seul type de calcul, alors que dans le second, semblable à ce que nous manipulons, l'architecture du code ou de l'algorithme est construite à volonté, ce qui est beaucoup plus complexe. La difficulté peut se lire dans le record de factorisation, atteint en 2012 par Enrique Martin-Lopez, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou et Jeremy L. O'Brien de l'université de Bristol, avec un dispositif quantique optique, qui consiste à factoriser le nombre $21 = 3 \times 7$ en exécutant l'algorithme de Shor.

Principe du fonctionnement d'un ordinateur quantique

Nous ne tenterons pas ici d'expliciter l'algorithme de Shor, mais simplement de donner quelques idées intuitives sur la façon dont un ordinateur quantique peut effectuer un calcul. Le principe de base est que le calcul doit pouvoir se ramener à une évolution hamiltonienne de l'état initial, suivie d'une « mesure » qui détermine l'état du q-registre, mais interrompt aussi son évolution. Conformément aux principes de la mécanique quantique, la valeur trouvée sera associée à un des états propres de l'observable mesurée, qui correspond ici à un état classique du registre, c'est à dire à un mot binaire. Pour pouvoir effectuer des opérations successives, l'hamiltonien qui régit le système évoluera au cours du temps, sous l'action d'une horloge qui détermine le rythme du calcul. À première vue, la détermination de ce hamiltonien semble être

19. Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. Texte en accès libre sur arXiv : quant-ph/9508027 (https ://arxiv.org/abs/quant-ph/9508027).

un problème inextricable si l'on souhaite effectuer un calcul non trivial. En fait, on montre que cette construction peut être menée à bien de façon relativement simple, car un calcul réel peut être décomposé en une succession d'opérations simples n'affectant qu'un ou deux bits. Ces opérations simples sont effectuées par des « portes logiques », dont des exemples bien connus classiquement sont les portes *NON*, *ET*, *OU*,... Les portes quantiques requises par l'algorithme de Shor présentent certaines particularités :

— elles doivent être « réversibles », car découlant d'une évolution hamiltonienne des bits d'entrée ;

— elles doivent manipuler des q-bits, sur lesquels on peut effectuer certaines opérations logiques inconcevables classiquement.

Un exemple simple de porte quantique est la porte $\sqrt{NON}$, qui prépare un q-bit dans une superposition linéaire à poids égaux des valeurs 0 et 1 (c'est une rotation de $\pi/2$ pour un spin 1/2). Il faut appliquer deux fois cette porte pour inverser 0 et 1 (porte *NON*), d'où le nom de porte $\sqrt{NON}$.

On pourrait penser qu'il suffit ensuite de faire évoluer l'ordinateur vers un état à une seule composante, qui serait la valeur recherchée. En fait, très peu d'algorithmes se prêtent à une manipulation aussi simple. L'état final de l'ordinateur est en général encore une superposition linéaire, et le résultat obtenu est donc aléatoire. Par exemple, si l'on considère l'algorithme de Shor, le résultat obtenu doit plutôt être considéré comme un « indice » permettant la factorisation ; il est facile de vérifier par un moyen conventionnel si la réponse est la bonne, et de relancer le calcul si non. Peter Shor a montré que cette procédure d'essai-erreur fournit la bonne réponse avec une probabilité arbitrairement proche de un, si l'on effectue un nombre d'essais croissant linéairement avec le nombre de chiffres du nombre à factoriser, et non plus exponentiellement.

La décohérence

Le principe d'un ordinateur quantique est donc compatible avec les lois de la physique, et un tel ordinateur semble réalisable, du moins tant que l'on considère des calculs simples, ne faisant intervenir qu'un petit nombre de portes.

Rappelons que le prix Nobel de physique 2012 a été décerné conjointement à Serge Haroche et à David Wineland "Pour des méthodes expérimentales révolutionnaires permettant de mesurer et de manipuler des systèmes quantiques individuels", notamment pour l'observation et le maintien des q-bits. (voir le chapitre 4.6).

Lorsqu'on atteint des tailles de calcul importantes, l'état global de l'ordinateur se présente comme une superposition linéaire d'un très grand nombre d'états, dont l'évolution doit être contrôlée tout en préservant toutes les propriétés de la superposition linéaire. Il n'est pas clair à l'heure actuelle que ce type de système est réalisable en pratique, et les recherches portent essentiellement dans deux directions :

— d'une part, il faut que le q-registre en évolution soit extraordinairement bien isolé de l'environnement extérieur. Tout couplage avec cet environnement va en effet induire un effet de « décohérence », susceptible de brouiller la superposition linéaire (comme pour le chat de Schrödinger).

— d'autre part, il faut prévoir en cas de perturbation des « codes de correction d'erreurs » capables de remettre l'ordinateur dans l'état qui était le sien avant l'action de la perturbation extérieure.

Ces deux voies - choix du système et codes de correction - sont très activement étudiées, et les questions soulevées ont stimulé aussi bien l'algorithmique que la physique quantique expérimentale. Il est actuellement très difficile de prévoir l'issue de ces recherches, mais il est tout à fait envisageable que des opérations logiques simples trouvent à moyen terme des applications dans les systèmes de cryptographie quantique.

Résultats actuels

Les concepteurs de q-bits travaillent dans plusieurs directions.
La plus ancienne est l'utilisation d'ions, des atomes débarrassés d'un ou de plusieurs électrons, piégés dans un système d'ondes stationnaires laser. Un problème est que l'adjonction d'un q-bit supplémentaire à un système qui fonctionne déjà est d'une grande difficulté car elle oblige à tout reconstruire pour des raisons géométriques complexes.
Un secteur prometteur repose sur la jonction Josephson, un composant supraconducteur refroidi près du zéro absolu, qui a notamment été l'objet de résultats marquants au CEA dans le groupe de Daniel Estève [20]. Il est relativement facile d'interconnecter de tels circuits pour créer des composants complexes.
Une autre technique utilise les atomes provenant d'un condensat de Bose-Einstein piégés dans un réseau optique.
Une dernière voie consiste en l'utilisation de *boîtes quantiques* de deux types principaux. L'un, appelé système d'atomes artificiels, s'appuie sur des semi-conducteurs comme l'arséniure de gallium, l'autre s'appuie sur une propriété des spins dans des structures nanométriques : la spintronique. Ces voies semblent prometteuses.

L'ordinateur quantique est un domaine de recherche bouillonnant à l'heure actuelle dans le monde entier. La littérature est plus qu'abondante. Le MIT, pour sa part, a placé en libre accès un outil d'aide à l'architecture de circuits quantiques (théoriques) simples [21]. Des chercheurs ont également exploré un domaine d'ordinateurs mixtes partiellement classiques et partiellement quantiques [22].

Mentionnons quelques étapes. Il existe, bien sûr, des querelles de rivalité, liés au secret évident sur les processeurs eux-mêmes. L'entreprise D-Wave Systems, basée en Colombie-Britannique, qui s'est présentée comme première entreprise d'informatique quantique au monde, ayant annoncé en 2007 avoir construit le prototype d'un processeur de 28 q-bits, a déclaré en 2011 qu'elle avait réussi à mettre au point le système "D-Wave One" comme le premier calculateur quantique commercial. Ce serait un processeur de 128 q-bits, et, en 2016, elle a fait un communiqué sur sa prochaine

20. François Mallet, Florian R. Ong, Agustin Palacios-Laloy, François Nguyen, Patrice Bertet, Denis Vion et Daniel Esteve, *Single-shot qubit readout in circuit quantum electrodynamics*, Nature Physics **5**, pages 791-795 (2009)

21. On les trouvera sur le site http ://www.media.mit.edu/quanta/qasm2circ/

22. Vedran Dunjko, Yimin Ge, and J. Ignacio Cirac, *Computational Speedups Using Small Quantum Devices*, Phys. Rev. Lett. **121**, 250501, 2018

génération de processeurs contenant 2000 q-bits, ce qui semble considérable. Plusieurs experts sont dubitatifs.

Google [23], reprenant ses propres recherches, interrompues en 2014, a présenté en 2018 *Bristlecone*, son premier processeur quantique intégrant 72 q-bits, lors de la réunion annuelle de l'American Physical Society à Los Angeles. La supériorité de ce nouveau composant ne réside pas seulement dans son nombre de q-bits, mais aussi dans un taux d'erreur particulièrement faible. Si les prévisions sont correctes, Bristlecone serait le premier processeur à dépasser le seuil dit de "suprématie quantique" estimé à 50 q-bits, au-delà duquel aucun super ordinateur classique ne serait capable de rivaliser avec son équivalent quantique.

Les physiciens Chinois sont des participants actifs dans cette course, à laquelle participent Atos, Intel, et IBM qui a réussi en 2017 à simuler la structure moléculaire de l'hydrure de béryllium (BeH2) sur un ordinateur quantique. Ces travaux ont démontré la capacité, annoncée par Feynman, des ordinateurs quantiques pour déterminer les états moléculaires. L'espoir est d'aboutir à la structure et la fonction des protéines. La médecine devrait, à terme, bénéficier grandement du développement des calculateurs quantiques.

16.5 Les « métiers » quantiques

On devine que ces développements scientifiques et technologiques ont suscité des investissements importants tant dans les grandes entreprises qu'au niveau des États et institutions internationales. Certaines agences de presse ont appelé cet élan une "Course internationale autour de la physique quantique", ce qui n'est pas faux.

La Chine en est un exemple frappant. Le développement est dû à la progression de l'économie dans ce pays et à un investissement massif dans la recherche fondamentale, qui a commencé dès le début des années 2000 avec la formation de nombreux chercheurs à l'étranger, en Europe, aux États-Unis et au Japon, chercheurs qui, revenus dans leur pays, y ont trouvé les moyens de développer des activités de pointe. Nous avons déjà mentionné le rôle essentiel de Jian-Wei Pan, formé en 1996 par Anton Zeilinger en Autriche, qui a développé plusieurs centres de recherche fondamentale et appliquée à Shanghai. Nous avons donné quelques exemples de l'activité de son groupe, qui a largement essaimé dans d'autres instituts chinois. À titre d'exemple, Jian-Wei Pan, et la direction chantier naval CSIC (China Shipbuilding Industry Corporation) créé en 1999, ont créé un laboratoire commun "Les communications quantiques, la navigation quantique et les radars quantiques". C'est un exemple des ambitions affichées par la Chine dans des domaines jusque-là dominés par les États-Unis, le Canada et l'Europe. La Chine a annoncé un investissement de 10 milliards de dollars dans la cryptographie quantique, et un effort de même ordre dans l'ordinateur quantique. Il est probable que c'est dans le domaine de l'informatique que la Chine a un retard quantitatif quant au nombre de spécialistes dans les secteurs en développement.

Il est plus difficile de donner l'ordre de grandeur, certainement équivalent, de l'investissement aux États-Unis, pour plusieurs raisons. Cet investissement se trouve dans les grandes entreprises comme IBM, Google, Microsoft, Intel, les géants de la Silicon

23. https ://www.tomshardware.fr/2018/03/06/bristlecone

Valley, mais aussi l'impressionnant réseau de centres universitaires de très haut niveau, MIT, Caltech, Stanford, Harvard etc. dont certains projets sont financés par des institutions fédérales, et qui savent transférer les recherches fondamentales et les technologies associées vers l'ingénierie. Il va sans dire que beaucoup de recherches sur les technologies quantiques se font dans un secret absolu, tant dans l'industrie que dans la défense, et la part de l'investissement Fédéral est impossible à évaluer. Au Canada, que nous avons évoqué ci-dessus, le secteur quantique est développé depuis déjà vingt ans. On estime à un milliard de dollars l'investissement fait pendant cette période, notamment dans l'Ontario où la "Vallée quantique de Waterloo" a vu se multiplier toute une série de recherches appliquées et de développements technologiques, notamment à l'Institute for quantum computing[24]. On s'attend, là aussi, à de gros investissements dans la prochaine décennie.

En Europe, si le nombre et la qualité des instituts et centres de recherche sont connus, il est admis que la transition des travaux et projets vers l'entreprise et l'industrie se fait mal. On sait que l'on forme d'excellents spécialistes, mais il existe une difficulté à transférer cette compétence vers les applications. Les analystes s'accordent à dire que cela n'est pas un problème de qualité de la recherche, mais d'industrialisation. "On lève facilement les premiers millions mais, dès qu'il s'agit de lever un capital de croissance, avec des sommes et un risque plus importants, tout se complique" dit Grégoire Ribordy, fondateur de la société genevoise ID Quantique. Pour répondre à la question : "L'Europe relèvera-t-elle le défi des technologies quantiques ?", l'Union Européenne a pris la décision d'investir, à partir de 2019, un milliard d'euros dans les dix prochaines années pour la recherche sur les technologies quantiques. Lancé en octobre 2018, le projet *Quantum Flagship*[25] fait suite aux deux programmes de recherche européens précédents : *Human Brain Project* et *Graphene Flagship*, visant à développer les technologies du futur. Il concerne plus de 5000 chercheurs. On trouvera tous les détails sur ce projet sur *https ://qt.eu/*. Si l'investissement peut paraître faible par rapport aux programmes chinois ou américains, il faut bien comprendre que l'objectif primordial est d'amener l'Europe à occuper un rôle de leader de cette aventure scientifique et technologique. Dans cette optique, on doit doter les groupes de recherche en pointe de moyens adaptés pour être à même d'inventer et de mettre au point des technologies, puis de participer avec des entreprises allant de start-ups à de grosses entreprises, voire des institutions européennes, à la R&D d'installation de ces technologies. Le milliard d'euros de l'UE doit avoir un effet d'entraînement, et devrait générer au moins 5 à 6 milliards de financements publics et autant du secteur privé. Les premiers domaines choisis portent sur : le Calcul quantique, la Communication quantique, les Simulations quantiques, les Capteurs et la Métrologie quantique, et la "Science fondamentale" quantique. Parmi les 140 projets proposés à la Commission, 20 ont été sélectionnés dans la première étape, avec une allocation globale de 140 millions d'euros pour 3 ans, parmi lesquels on notera plusieurs projets suisses, dont on connaît par ailleurs la qualité, L'Université de Genève, le Centre Suisse d'électronique et de microtechnique à Neuchâtel, L'ETH de Zurich et l'Université de Bâle.

24. https ://uwaterloo.ca/institute-for-quantum-computing/
25. Quantum Technology — The future is Quantum, https ://qt.eu/

Quant aux *métiers quantiques*, il faut bien admettre qu'ils posent problème, étant donné la formation qu'ils exigent. Dans ce domaine, le "recyclage" est permanent, comme dans la recherche fondamentale, il ne s'improvise pas. Trouver des ingénieurs spécialistes de l'informatique quantique, de la téléportation ou de quelque autre spécialité de ces domaines, n'est pas chose aisée. On conçoit que cette question ait en Europe des résonances que l'on trouve avec moins d'ampleur en Chine ou aux États-Unis (pour des raisons très différentes dans ces deux pays). Certains disent que c'est un peu chercher un mouton à cinq pattes, tant les profils sont rares : il faudrait, sur le papier, recourir à des mathématiciens appliqués, des physiciens de divers domaines, des ingénieurs pour faire fonctionner le matériel, des informaticiens pour inventer les codes, et des animateurs capables de faire travailler tout ce beau monde ensemble. Pourtant c'est bien ce que l'on fait quotidiennement dans la recherche fondamentale. La différence est que ces métiers quantiques font appel à des capacités de communication transversale, d'un domaine à un autre, qui sont peu sinon pas pratiquées dans la recherche fondamentale française. C'est là un aspect culturel probablement aussi important que les réussites pratiques sur tel ou tel thème.

L'information quantique, qui termine ce livre, est en train de devenir une retombée prodigieuse de la mécanique quantique. Un simple aperçu de la littérature sur le sujet montre tout de suite que c'est là un vaste domaine de recherche scientifique et technologique, un sujet en soi. Tous ces développements sont impressionnants, par eux-mêmes, par leur thème et par leurs buts. Mais ce qui est probablement encore plus étonnant est qu'ils aient pris racine dans des interrogations intellectuelles soulevées par Einstein en 1935, et façonnées par quelques orfèvres comme John Bell. Un progrès technologique considérable est en train de se construire à cause de *paradoxes intellectuels* ! Cette explosion technologique s'est produite à la suite de résultats théoriques et expérimentaux des années 1970 et 1980, conçus pour obtenir un accord sur la question : Comprenons-nous la mécanique quantique ? Il n'y a toujours pas de réponse complète [10], [30].

Quant aux *métiers quantiques*, il faut bien admettre qu'ils posent problème, étant donné la formation qu'ils exigent. Dans ce domaine, le "recyclage" est permanent, comme dans la recherche fondamentale, il ne s'improvise pas. Trouver des ingénieurs spécialistes de l'informatique quantique, de la téléportation ou de quelque autre spécialité de ces domaines, n'est pas chose aisée. On conçoit que cette question ait en Europe des résonances que l'on trouve avec moins d'ampleur en Chine ou aux États-Unis (pour des raisons très différentes dans ces deux pays). Certains disent que c'est un peu chercher un mouton à cinq pattes, tant les profils sont rares : il faudrait, sur le papier, recourir à des mathématiciens appliqués, des physiciens de divers domaines, des ingénieurs pour faire fonctionner le matériel, des informaticiens pour inventer les codes, et des animateurs capables de faire travailler tout ce beau monde ensemble. Pourtant c'est bien ce que l'on fait quotidiennement dans la recherche fondamentale. La différence est que ces métiers quantiques font appel à des capacités de communication transversale, d'un domaine à un autre, qui sont peu sinon pas pratiquées dans la recherche fondamentale française. C'est là un aspect culturel probablement aussi important que les réussites pratiques sur tel ou tel thème.

L'information quantique, qui termine ce livre, est en train de devenir une retombée prodigieuse de la mécanique quantique. Un simple aperçu de la littérature sur le sujet montre tout de suite que c'est là un vaste domaine de recherche scientifique et technologique, un sujet en soi. Tous ces développements sont impressionnants, par eux-mêmes, par leur thème et par leurs buts. Mais ce qui est probablement encore plus étonnant est qu'ils aient pris racine dans des interrogations intellectuelles soulevées par Einstein en 1935, et façonnées par quelques orfèvres comme John Bell. Un progrès technologique considérable est en train de se construire à cause de *paradoxes intellectuels* ! Cette explosion technologique s'est produite à la suite de résultats théoriques et expérimentaux des années 1970 et 1980, conçus pour obtenir un accord sur la question : Comprenons-nous la mécanique quantique ? Il n'y a toujours pas de réponse complète [10], [30].