Physique pour tous

Cours 11 : *Mécanique Quantique IV*

Antoine Tilloy [*] [†]

Résumé

Notes [1] du dernier cours de mécanique quantique. On y parle de la non-localité démontrée par Bell et des applications de la théorique quantique au calcul et à la cryptographie.

1 Théorème de Bell

1.1 Introduction

Au cours précédent, nous avons vu que beaucoup de caractéristiques de la mécanique quantique qui semblent a priori inévitables (impossibilité des trajectoires, indéterminisme intrinsèque de la Nature) dépendent en réalité largement de l'interprétation que l'on fait du formalisme. Il existe une caractéristique de la nature, prédite par la mécanique quantique, qui est réellement indépendante de l'interprétation : c'est la *non-localité*, démontrée par Bell en 1964 [2].

Sachant qu'il y a eu d'infinies controverses, incompréhensions et même contresens autour du résultat de Bell –le théorème ayant été lié à la notion vague de «réalisme»– il est nécessaire de préciser ce qui a amené Bell à se poser la question de la non-localité. Au début des années 1950, John Bell découvre la théorie de l'onde pilote (dBB) développée à l'époque par David Bohm et est fasciné par ses propriétés. Il observe que, contrairement à ce que l'on prétendait à l'époque, la mécanique quantique n'est pas incompatible avec l'existence d'une réalité objective indépendante de l'observation. En fait, la supposée impossibilité de la réalité avait été «démontrée» par Von-Neumann. En étudiant dBB, contre exemple au théorème, Bell comprend la faille du raisonnement de Von-Neumann et de ses successeurs [2]. Cependant, si dBB rend bien compatible avec la mécanique quantique la notion usuelle de réalité (ici simplement des particules ponctuelles qui bougent) elle possède une caractéristique désagréable : la non-localité. En effet dans dBB des particules éloignées s'influencent de manière instantanée via la fonction d'onde, des régions très éloignées de l'espace semblent bizarrement connectées. Bell pense alors que comme beaucoup de caractéristiques, cette non-localité n'est qu'apparente et contingente à l'interprétation. Il entreprend alors de construire une théorie locale, qui garderait le réalisme de dBB sans avoir cette bizarrerie non-locale. Comme d'habitude, Bell cherche à réduire le romantisme de la théorie au maximum pour qu'il n'y ait pas plus de bizarrerie dans le formalisme qu'il n'y en a dans la Nature qu'il modélise. Bell se rend rapidement compte que son entreprise est impossible : imposer la localité est impossible, car si la Nature obéit aux prédictions de la mécanique quantique, alors elle est nécessairement non-locale.

Ce résultat a souvent été mal interprété, au grand dam de Bell, comme démontrant l'impossibilité du réalisme, ou plutôt comme imposant de faire un choix entre réalisme et localité. On [3] décrète alors que la non-localité est inacceptable et on en conclut tout fier

[*]Laboratoire de Physique Théorique, École Normale Supérieure, Paris
[†]contact : tilloy@lpt.ens.fr

1. Dernière modification : 15 janvier 2016
2. Bell explique l'erreur de Von-Neumann dans un article de revue ultérieur [1]
3. Ce «on» contient malheureusement beaucoup de physiciens respectables...

qu'il n'y a pas de réalité [4]. En réalité Bell cherche à montrer l'exact opposé. Dans tous les cas, la Nature est non-locale. Dès lors le prix de la réintroduction de la «réalité» n'est pas, comme on le pensait, la perte de la localité. La réalité vient gratuitement. Le défaut a priori rédhibitoire de dBB, la non-localité, n'en est plus un, puisqu'il est nécessairement partagé par les autres interprétations, fusse de manière cachée.

1.2 Inégalité de Bell

Il existe une multitude de manières d'écrire les inégalités de Bell possédant chacune des degrés variables de généralité. Sachant que notre seul objectif sera de démontrer qu'une inégalité est violée par la mécanique quantique (et l'expérience), la généralité n'est pas utile (du moins d'un point de vue logique) ; il nous suffit de regarder un exemple simple. Ce cas particulier de l'inégalité de Bell s'appelle parfois l'inégalité de Wigner et on peut en trouver d'excellentes présentations dans Bricmont [4] ou Laloë [5].

Rappelons tout d'abord que l'inégalité de Bell est une inégalité entièrement classique (c'est à dire une inégalité sur des probabilités), inutile de connaître la mécanique quantique. On va considérer une situation (presque un jeu) «classique» dans lequel des individus doivent répondre à des questions et démontrer une certaine relation sur les fréquences de leur réponses.

On considère un jeu ou une sorte d'interrogatoire auquel vont être soumis 2 individus. Cet interrogatoire comporte 3 questions que l'on va appeler A, B et C (par exemple A = «Avez vous aimé *Eden* ?»). On suppose que ces questions n'admettent que des réponses binaire («Oui» ou «Non»). Initialement, les deux individus peuvent discuter, établir des stratégies arbitrairement subtiles. Puis on les éloigne l'un de l'autre, l'un reste dans un bunker sur Terre, l'autre est envoyé dans un bunker sur une planète à l'autre bout de la galaxie. On leur pose alors à chacun une question qui n'est pas forcément la même, par exemple B à l'individu sur Terre et A à l'individu à l'autre bout de la galaxie. On effectue l'intégralité de cette séquence (les individus choisissent une stratégie, s'éloignent, on leur pose à chacun une question aléatoire) un nombre très grand de fois en notant les résultats. Le résultat d'une expérience donnée est de la forme *«Le premier individu a tiré la question A et a répondu «oui», le second a tiré la question C et a répondu «non»*.

On a ajoute ensuite une règle. Lorsque par hasard la même question est posée aux deux individus, alors il doivent répondre la même chose. Cette règle contraint fortement les stratégies possibles. On voit typiquement que la stratégie qui consisterait à répondre au hasard ne fonctionne pas. En fait, et c'est le point essentiel, il faut se convaincre que la seule stratégie possible (ou disons le sous ensemble de stratégies possibles) est de se mettre d'accord sur une réponse déterminée à chaque question. En effet, dans leur bunker ils ne pourront plus communiquer, si les individus ne se sont pas mis d'accord à l'avance sur les réponses à chaque question il arrivera forcément un moment où, alors qu'on leur a posé la même question (sur Terre et à l'autre bout de la galaxie), ils ne répondront pas la même chose (ce qui est interdit par la règle). La situation est assez analogue à celle d'un vrai interrogatoire séparé de deux criminels.

L'idée de Wigner est ensuite de regarder le sous ensemble des situations où des questions différentes sont posées à chaque individu (par exemple A sur Terre et C à l'autre bout de la galaxie). Dans ce cas, qu'elle est la probabilité que les deux individus répondent quand même la même chose (i.e. tous les deux «oui» ou tous les deux «non»). Wigner remarque que les individus sont quand même d'accord en moyenne dans au moins 1 cas sur 3. C'est en fait assez facile à vérifier. Le sous ensemble des stratégies dans lesquelles les individus se mette d'accord sur la réponse à donner à chaque question contient exactement $2^3 = 8$ stratégies (oui ou non à chaque réponse). Il y a essentiellement deux sous classes de stratégies, soit la réponse à toutes les questions est la même (A : oui, B : oui, C : oui, ou l'inverse), soit une réponse est différente des deux autres (par exemple A : oui, B : non, C : non). Dans le premier cas, les individus sont tout le temps d'accord quelle que soit la question, la probabilité vaut 1. Dans le second cas on peut considérer l'exemple précédent. Si le premier individu a eu la question A, alors, comme on regarde

4. Même si le présupposé qu'il fallait choisir entre réalité et localité était vrai, la conclusion qu'il faudrait alors privilégier la localité semble assez ridicule.

les sous cas où les deux individus ont eu des questions différentes, l'autre a eu B ou C il ne répondra pas la même chose. Si le premier individu a eu la question B, alors l'autre a eu forcément A ou C et répondra la même chose avec probabilité 1/2, de même si le premier individu a eu la question C. Finalement la probabilité que les deux individus répondent la même chose dans cette stratégie vaut $p = 1/3$. Les autre cas se traitent de manière analogue. Finalement on obtient ce résultat :

$$Prob(\text{même réponse} \,|\, \text{question différente}) \geq \frac{1}{3}$$

Ce résultat peut paraître extrêmement trivial. Quel est donc le rapport avec la physique ? On n'a l'impression de n'avoir absolument rien supposé sur le monde physique à part l'impossibilité de communication quand les deux individus sont très éloignés [5]. En fait ce résultat banal est suffisant pour démontrer le théorème de Bell : la mécanique quantique permet que la probabilité précédente soit exactement égale à 1/4 !

1.3 Violation quantique

Prouver que la relation précédente peut être violée en mécanique quantique n'est pas très difficile mais dépasse (de presque rien) le niveau de ce cours. On peut néanmoins en donner l'idée générale. On considère deux boîtes contenant chacune deux compartiments. Il y a une particule dans chaque boîte et la seule information que l'on retient est de savoir dans quel compartiment est la particule. Ensuite on produit [6] un état intriqué (à la EPR) de ces deux particules. Chaque individu prend avec lui une des boites contenant une particule mais qui reste quantiquement intriquée avec l'autre. Ensuite, on peut montrer qu'en associant à chaque question A, B ou C une certaine succession évolution-mesure sur la particule dans la boite et en associant au résultat de cette mesure une réponse binaire «oui» ou «non», les individus peuvent effectivement répondre la même chose lorsqu'on leur pose la même question, mais avoir une probabilité d'être en accord dans les autres cas de 1/4 seulement ce qui viole l'inégalité de Bell (dont un cas particulier est l'inégalité de Wigner). C'est l'intrication qui permet cette violation d'une inégalité qui semble pourtant être une évidence. Cette expérience a été réalisée par Alain Aspect en 1981 en remplaçant les boites par des photons et les compartiments par des états de polarisation de ces photons. Les détails importent peu, il suffit de savoir que bien que les objets physiques soient différents, la situation est en fait exactement la même. En fait, Alain Aspect testait aussi une inégalité un peu différente de celle de Wigner, mais pour simplifier (simplification qui n'enlève rigoureusement rien au raisonnement), on peut dire qu'il a indirectement mesuré la probabilité précédente et qu'il a trouvé :

$$Prob(\text{même réponse} \,|\, \text{question différente}) \simeq 0.25 \pm 0.01 < \frac{1}{3}$$

Ainsi, aux erreurs expérimentales près, non seulement l'inégalité de Bell est violée, mais la violation est exactement celle qui est prédite par la mécanique quantique.

1.4 «*No faster-than-light signalling*»

Le théorème de Bell montre qu'il existe une forme d'action instantanée à distance dans la Nature. C'est à première vue en contradiction directe avec ce que l'on a vu en relativité restreinte où on ne peut transmettre aucune information plus vite que la

5. Cette impossibilité semble raisonnable au moins avec la relativité restreinte. En effet, si les individus sont très éloignés l'un de l'autre et qu'on leur pose une question simultanément *dans le référentiel dans lequel ils sont au repos*, alors il est impossible qu'ils échangent de l'information pour se dire quelle question ils ont eu. Comme ces deux événements sont dans l'ailleurs l'un pour l'autre, il existe des référentiels en mouvement dans lesquels l'un arrive avant l'autre ou l'inverse ce qui interdit toute causalité entre les deux.

6. La question de savoir comment produire en pratique un état de particules intriqués dépasse le cadre de ce cours mais il faut insister sur le fait que c'est possible et réalisé chaque jour dans les laboratoire. Des états intriqués de photons sont même utilisés dans des applications commerciales de la cryptographie quantique.

lumière. En fait, il n'y a pas de contradiction dans les prédictions des deux théories (même s'il y a une tension évidente). La non-localité au sens de la mécanique quantique ne permet pas de transmettre de l'information. Dans l'expérience précédente, la non-localité permet aux deux individus de corréler leurs réponses, mais ils ne peuvent jamais savoir à quelle question l'autre est en train de répondre. La mécanique quantique ne peut pas permettre à un individu d'obtenir des informations sur l'autre instantanément. C'est uniquement lorsque l'on met à côté les réponses des deux individus que l'on découvre une corrélation qui n'est pas explicable sans la non-localité. En fait c'est un théorème général : la mécanique quantique ne permet pas de transmettre de l'information plus vite que la lumière même si elle peut créer des corrélations non-locales.

1.5 Ce que dit *vraiment* le théorème de Bell

Résumons ce que dit le théorème de Bell. Le théorème de Bell est un résultat *théorique* qui dit que toute théorie qui viole une certaine inégalité (l'inégalité de Bell) est forcément non-locale. La mécanique quantique viole par exemple cette inégalité et est donc non-locale. Expérimentalement, on mesure que l'inégalité est violée, la Nature est donc non-locale. Accessoirement, la violation prévue par la mécanique quantique est exactement celle que l'on observe expérimentalement.

En revanche le théorème de Bell ne dit

— rien sur l'indéterminisme supposé intrinsèque de la nature !
— rien sur l'impossibilité de la réalité.
— rien sur la possibilité de communiquer plus vite que la lumière (c'est toujours impossible).
— rien sur la télépathie et autres joyeusetés New-Age.

2 Applications à l'information quantique

Après tant de théorie, on a gagné le droit de se détendre avec les applications de la mécanique quantique. Il est toujours un peu délicat de savoir ce que l'on entend par applications de la mécanique quantique. En effet, la mécanique quantique décrit a priori tous les phénomènes et modifie significativement les prédictions classiques pour une large classe de systèmes mésoscopiques. Des effets purement quantiques rendent possible le laser et le transistor à semi-conducteur qui constituent les deux piliers de la technologie moderne (Internet et ses fibres optiques, les ordinateurs, les smartphones, et enfin presque tout ce qui contient de l'électronique). Je souhaite plutôt présenter deux applications de la mécanique quantique qui utilisent explicitement sa non-localité et donc la quintessence de sa différence avec la physique classique. Ces applications appartiennent à ce que l'on appelle en général la deuxième révolution quantique : l'ordinateur quantique et la cryptographie quantique.

2.1 Quelques éléments de cryptographie classique

Avant de parler de son analogue quantique, il est nécessaire d'expliquer comment fonctionne la cryptographie à clé publique standard qui est déjà assez astucieuse.

La cryptographie à laquelle on pense naïvement est la cryptographie à clé privée. Alice et Bob possèdent chacun la même clé avec laquelle ils cryptent leur message. Une clé peut-être typiquement une longue liste de nombres. Pour crypter leur message, Alice et Bob décalent la première lettre du message de n_1 lettres dans l'alphabet où n_1 est le premier chiffre de la clé dans, puis font de même avec la deuxième lettre, etc. Par exemple :

$$\text{Message : } H-E-L-L-O + \text{ Clé : } 1-2-4-3-1 \longrightarrow \text{Message crypté : } I-G-P-O-P$$

Si la clé est aussi longue que le message, alors l'encodage est parfait et incassable car le message crypté ne contient pas plus d'information qu'une suite de lettres aléatoires

pour celui qui n'a pas la clé. Le problème de cette procédure c'est qu'Alice et Bob doivent partager une clé sûre au départ. C'est la partie critique, il est très difficile de s'assurer que personne n'a pu se procurer la clé à une moment ou à un autre. De plus on ne peut pas s'envoyer la clé, il faut trouver un moyen de se retrouver physiquement pour se donner la clé, seul moyen d'être être sûr que personne ne l'a interceptée.

Il existe une autre méthode de cryptographie moins intuitive et qui en fait celle qui sécurise la plus grande partie des échanges notamment sur internet, la cryptographie à clé publique. Commençons par une explication avec les mains. L'idée de la cryptographie à clé publique est la suivante. Alice possède un coffre fort à clé, elle envoie le coffre fort ouvert à Bob sans la clé. Bob met son message dans le coffre fort et le ferme, opération qui ne demande pas d'avoir la clé. Le coffre fort, supposé inviolable sans la clé est alors renvoyé à Alice qui peut l'ouvrir. On comprend que cette méthode ne demande pas de partager une quelconque information au départ. Évidemment en pratique, on n'utilise pas un coffre fort physique mais un analogue mathématique.

L'idée est de posséder une fonction mathématique à sens unique qui permette de crypter un message mais pas de le décrypter sauf si on possède une clé supplémentaire :

$$\text{Message} \xrightarrow{f} \text{Message crypté}$$
$$\text{Message crypté} \overset{f}{\not\to} \text{Message}$$
$$\text{Message crypté} \overset{f+\text{clé}}{\to} \text{Message}$$

La fonction f joue alors le rôle du coffre. En pratique on utilise des propriétés remarquables de l'arithmétique des nombres premiers pour construire une telle fonction. Dans ce qui suit je vais donner l'idée de l'algorithme RSA qui sert à chiffrer la plupart des transmissions d'informations sensibles sur Internet.

Alice choisit deux gros nombres premiers p et q qu'elle multiplie pour obtenir $n = pq$. Elle envoie le nombre n à Bob. Bob applique ensuite une transformation mathématique à son message qui dépend de n (pour plus de détails sur la transformation qui utilise des congruences, on peut consulter l'article Wikipedia sur RSA) et produit un message crypté. Pour décrypter le message, il faut connaître la décomposition de n i.e. p et q, avec seulement n c'est impossible. Alice qui les connaît peut lire le message. Le nombre n étant public, si Eve a intercepté le message crypté et souhaite le lire, il lui «suffit» de factoriser n pour en sortir la clé c'est à dire p et q. Le problème, c'est que c'est difficile pour des grands nombres : on ne connaît aujourd'hui aucun algorithme permettant d'effectuer cette opération rapidement, ce qui protège la méthode. On peut rendre p et q suffisamment grand pour que cette tâche ne soit pas accessible même aux plus puissants super calculateurs actuels.

2.2 Ordinateur quantique et théorie de la complexité

Commençons par faire un petit détour par la théorie de la complexité en informatique. Il existe deux classes de problème intéressants en informatique théorique. La première est la classe «P» des problèmes dont on peut *trouver* la solution en temps polynomial (c'est à dire intuitivement en un temps raisonnable qui ne croit pas exponentiellement avec la taille du problème) avec un ordinateur classique. Ce sont les problèmes gentils. La seconde est la classe des problèmes «NP» dont on peut vérifer la solution en temps polynomial. Si on me donne la solution d'un problème NP alors je sais dire rapidement si elle est correct ou non. En revanche, rien ne me dit a priori que j'aurais été capable de la trouver rapidement. On a naturellement que P est inclus dans NP, si je sais trouver la solution vite c'est que je peux la vérifier encore plus vite. Il existe évidemment d'autres classes de complexité, notamment celle des problèmes dont on ne peut même pas vérifier la solution rapidement mais on ne va pas s'en occuper. La question fondamentale de l'informatique théorique [7] est de savoir si P=NP ou P≠NP. A priori on a envie de dire que P est forcément différent de NP, il doit exister des problèmes dont il est facile de

7. Qui est une question du millénaire à un million de dollars de l'institut Clay.

vérifier la solution mais difficile de la trouver au départ. Il est probable que ce soit vrai, c'est d'ailleurs ce que pensent la majorité des informaticiens et mathématiciens, mais on n'a jamais réussi à le prouver en général. Quand on dit qu'un problème est NP, c'est donc que l'on n'a pas encore trouvé de méthode pour le résoudre rapidement, mais il n'existe pas de preuve fondamentale qu'un jour on n'y arrivera pas.

Cela nous amène à la factorisation d'un gros nombre n en produit de nombres premiers. On pense aujourd'hui qu'il s'agit d'un problème NP qui n'est pas dans P. Si on me donne deux nombres p et q (la solution du problème de factorisation) alors je sais dire très vite si leur produit vaut bien n et donc s'il s'agit d'une solution valable. En revanche, si on me donne seulement n et que ce n est grand, même avec des années de calculs sur d'énormes supercalculateurs, il est difficile de trouver p et q (une méthode naïve consiste à tester toutes les possibilités, mais si n est grand il y en a beaucoup). La plupart des gens pensent que ce problème restera à jamais difficile, du moins pour un ordinateur classique.

On a vu précédemment que la mécanique quantique possédait des différences fondamentales avec la physique classique. Sans rentrer dans les détails, on s'est rapidement rendu compte que la bizarrerie quantique (notamment la non localité) rendait extrêmement difficile (voire impossible en pratique) la simulation de processus physiques quantiques sur un ordinateur. C'est Richard Feynman qui a eu en premier l'idée de renverser le raisonnement et de conclure du précédent problème qu'il devait être possible d'exploiter la physique quantique pour résoudre des problèmes difficiles. On sait depuis les années 1980 que l'on peut réaliser un nouveau type d'ordinateur qui exploite des effets quantiques pour être plus rapide qu'un ordinateur classique. La révolution arrive en 1994 avec Peter Shor qui démontre qu'en utilisant un ordinateur quantique, il est possible de factoriser un gros nombre n en produit de nombres premier rapidement, c'est à dire de passer d'un problème que l'on croit classiquement dans NP (et pas dans P) à BQP (les problèmes dont on peut trouver rapidement la solution avec un ordinateur quantique). On pense aujourd'hui, même s'il n'en existe pas de preuve formelle, qu'aucune de ces catégories n'est incluse dans une autre. Autrement dit, on pense qu'il existe des problèmes qui appartiennent à BQP, NP mais pas P (comme la factorisation en nombres premiers par exemple) et des problèmes NP qui n'appartiennent pas à BQP (et donc pour lesquels l'ordinateur quantique n'apporte rien).

Pour revenir au problème de la factorisation des nombres premiers, si la technologie permet un jour effectivement de fabriquer un ordinateur quantique, alors l'algorithme RSA ne sera plus sûr car on pourra déduire p et q de n en un temps court. Actuellement de nombreuses équipes [8] se sont lancées dans la course à l'ordinateur quantique et il paraît possible sinon probable que des ordinateurs quantiques efficaces –typiquement capables de casser RSA– existent d'ici une vingtaine d'années.

2.3 Cryptographie quantique

De manière assez inattendue, la mécanique quantique apporte en même temps le remède à la destruction de la cryptographie classique à clé publique. La manière dont on s'y prend est assez intéressante. La cryptographie quantique ne protège pas la clé pendant son transfert mais permet de savoir à coup sûr si quelqu'un a pu l'intercepter. Rentrer dans les détails demande un peu plus de technique que ce que l'on a vu pendant ce cours mais l'idée est de partager la clé en envoyant des photons un par un. Si Eve mesure les photons au milieu de la ligne alors elle induit une perturbation irréductible (à cause de la mécanique quantique) sur leur évolution future ce qui modifie les mesures ultérieures faites par Alice et Bob. Ces derniers peuvent ainsi détecter la présence de Eve et attendre qu'elle ne soit plus là pour échanger une nouvelle clé. Si la mécanique

8. Les participants à la course appartiennent aux grandes universités (Caltech, MIT, Berkeley,...), au privé (IBM, Google, DWave,...) et aux états (laboratoires nationaux de Sandia, Los Alamos, CEA,...). L'argent vient aux États-Unis principalement de la IARPA et de la DARPA, les agences gouvernementales qui financent la recherche sur l'«Intelligence» (en gros pour la NSA et CIA) et la défense (pour l'armée). Personne n'a envie de se retrouver avec un petit labo privé qui aurait construit un ordinateur quantique avant tout le monde et lirait toutes les communications cryptées en secret. Comme pour la bombe, il est inenvisageable de n'être pas le premier.

quantique est correcte, alors cette méthode de cryptographie est parfaite et à tout jamais incassable. Sa sécurité ne dépend pas de notre difficulté à imaginer des algorithmes de décryptage efficaces (comme pour la crypto standard), mais de la physique elle même.

À la différence du calcul quantique, la cryptographie quantique commence à être implémentée. Elle sécurise déjà les communications de banques suisses (plus pour des raisons d'image que pour la sécurité du protocole) et est quotidiennement expérimentée sur de longues distances par différentes équipes de recherche un peu partout dans le monde. Il est aujourd'hui même possible d'acheter, ou plutôt de se faire fabriquer une ligne quantique sûre entre deux points. Même si elle en est évidemment à ses débuts, la cryptographie quantique est d'ores et déjà testée et approche la phase de démocratisation. A posteriori, on peut se dire qu'on a eu de la chance qu'il soit si difficile de réaliser un ordinateur quantique en pratique et comparativement facile d'implémenter la cryptographie quantique !

C'en est fini pour la mécanique quantique. Ceux qui veulent en savoir plus en restant dans l'approche «non-romantique» et minimalement mystificatrice de ces notes peuvent consulter le tout nouveau livre de Jean Bricmont [3] dont j'ai pu lire une version préliminaire et qui m'a semblé excellent. D'un point de vue calculatoire, rien n'est à savoir pour l'examen dans la mesure où on n'a presque rien fait. Les implications logiques de la théorie, ce qu'elle dit et ne dit pas du monde, le lien subtile entre interprétations et algorithme orthodoxe, et plus généralement le «méta» autour de la théorie méritent en revanche peut-être un peu d'attention.

Références

[1] John S Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3) :447, 1966.

[2] John S Bell et al. On the einstein-podolsky-rosen paradox. *Physics*, 1(3) :195–200, 1964.

[3] Jean Bricmont. *Making sense of quantum mechanics*. Springer, 2016.

[4] Jean Bricmont, Hervé Zwirn, and Thierry Martin. *Philosophie de la mécanique quantique*. Vuibert, 2009.

[5] Franck Laloë. *Comprenons-nous vraiment la mécanique quantique ?* EDP sciences, 2013.

Appendice technique : Extension du formalisme

Jusqu'à maintenant, nous avons considéré la mécanique quantique d'une particule unique. Cette mini théorie contient déjà des subtilités intéressantes comme les interférences ou l'effet tunnel et permet de rendre compte de systèmes aussi fondamentaux que l'atome. Néanmoins elle n'est pas suffisante car elle ne contient pas toute la bizarrerie quantique, i.e. il existe des phénomènes très contre intuitifs supplémentaires qui ne se manifestent que lorsque l'on considère plusieurs particules en même temps. On pourrait penser qu'il suffit d'attribuer à chaque particule une fonction d'onde et de traiter ensuite chaque fonction séparément en lui appliquant les postulats d'évolution et de mesure. Il se trouve que la description quantique d'un ensemble de particules est en fait plus riche que cette simple addition. On fait en général le choix de basculer vers une formalisation très abstraite de la mécanique quantique lorsque l'on veut traiter ces situations. Nous allons ici faire le choix moins usuel de rester le plus près possible du formalisme à une particule. Cela rendra la description moins sobre mathématiquement mais probablement plus compréhensible, ce qui est au fond la seule chose qui compte en première approximation. Un petit avertissement tout de même, cette section est un peu plus difficile que les autres et il peut être nécessaire de passer un peu de temps à y réfléchir pour l'assimiler complètement.

.1 Postulats à plusieurs particules

Par soucis de clarté, nous allons donner les postulats de la mécanique quantique pour deux particules en indiquant lorsque ça n'est pas évident comment la construction se généralise à un nombre arbitraire. En fait, le cas à deux particules contient déjà une grande part sinon l'intégralité de ce qui apparaît d'intéressant quand on quitte le cas d'une particule unique.

Commençons par fournir comme précédemment l'objet fondamental de la théorie. Il s'agit fort heureusement toujours d'une fonction d'onde. La différence cette fois-ci est que la fonction prend en argument les positions des deux particules :

Postulat (Fonction d'onde)**.** *L'état d'un couple de particules est contenu* intégralement *dans une fonction ψ qui prend comme arguments le temps t (nombre réel), la position x_1 (nombre réel) de la première particule, la position x_2 de la seconde et associe un nombre complexe :*

$$\psi : t, x_1, x_2 \longmapsto \psi(t, x_1, x_2)$$

La fonction d'onde est une fonction de la position des *deux* (ou des n si on en a un nombre n arbitraire) particules en même temps. Si l'on avait généralisé naïvement la mécanique quantique à une particule, on aurait été tenté de postuler l'existence de deux fonctions d'onde ψ_1 et ψ_2 pour chaque particule. Ce premier postulat fondamental dit au contraire que l'on est obligé de regrouper les deux, ce qui suggère déjà qu'il n'existe pas de description séparée de chaque particule. Il y a ainsi quelque chose de peu intuitif dans le formalisme : usuellement, on a l'habitude d'être capable de donner des propriétés à chaque sous système d'un plus grand système. En mécanique quantique, ce n'est pas toujours possible, il arrive que l'on puisse parler de l'état d'un ensemble sans pouvoir parler de l'état de ses constituants. La définition suivante précise les situations dans lesquelles on peut le faire.

Définition 1 (Séparabilité)**.** On dit que l'état d'un système composé de plusieurs particules est *séparable* si la fonction d'onde de ce dernier peut s'écrire comme un produit de fonctions ne dépendant chacune que de la position d'une seule particule. Dans le cas à deux particules, cela signifie qu'il existe deux fonctions ψ_1 et ψ_2 telles que :

$$\psi(t, x_1, x_2) = \psi_1(t, x_1) \cdot \psi_2(t, x_2)$$

Lorsqu'un système comprenant plusieurs particules est décrit par une fonction d'onde séparable, alors la généralisation naïve de la mécanique quantique qui consiste à traiter toutes les particules séparément fonctionne. Il suffit alors d'appliquer à chaque fonction

d'onde ψ_1 et ψ_2 (que l'on peut alors associer à la première et à la deuxième particule) les postulats d'évolution et de mesure, on peut décrire les deux particules complètement indépendamment. Graphiquement par exemple, on peut se contenter de dessiner la fonction d'onde des deux particules. Ce concept a un intérêt (la définition n'est pas triviale) parce que toute fonction d'onde d'un système composite n'est pas forcément séparable :

Définition 2 (Intrication)**.** L'état d'un ensemble de particule est dit *intriqué* (entangled) si la fonction d'onde qui le décrit n'est pas séparable.

Un moyen de fabriquer un état intriqué est de prendre deux états séparables quelconques $\psi^a(t, x_1, x_2) = \psi_1^a(t, x_1) \cdot \psi_2^a(t, x_2)$ et $\psi^b(t, x_1, x_2) = \psi_1^b(t, x_1) \cdot \psi_2^b(t, x_2)$ et de les ajouter en utilisant le principe de superposition, i.e. de poser :

$$\begin{aligned}\psi(t, x_1, x_2) &= \psi^a(t, x_1, x_2) + \psi^b(t, x_1, x_2) \\ &= \psi_1^a(t, x_1) \cdot \psi_2^a(t, x_2) + \psi_1^b(t, x_1) \cdot \psi_2^b(t, x_2)\end{aligned}$$

Une telle fonction, dans le cas général, ne peut pas s'écrire comme un produit et correspond donc à un état intriqué. Pour une fonction d'onde d'un état intriqué, on n'a pas de décomposition simple entre ce qui dépend de la première particule et ce qui dépend de la seconde, on ne peut associer à chacune une fonction d'onde, tout est en quelque sorte mélangé, entrelacé (d'où le terme «entangled state» en anglais). Les états intriqués contiennent ce l'on appelle la non-localité de la physique quantique, c'est à dire le fait qu'il est impossible, dans certaines situations, de définir les propriétés d'agrégats d'objets au niveau de chaque objet. On va revenir en détails sur ce concept et sur ses implications physique dans la suite du cours. Dans l'immédiat, il nous faut donner un dernier théorème mathématique (c'est à dire qui d'un point de vue physique n'introduit pas de nouveaux postulats) nous permettant de décomposer une fonction d'onde en fonctions d'onde séparables.

Théorème (Décomposition d'un état intriqué)**.** *Une fonction d'onde ψ d'un état intriqué peut toujours s'écrire comme la somme (éventuellement infinie) de fonctions d'ondes séparables $\psi^{(i)}$, ce qui peut se retranscrire de manière compacte :*

$$\psi = \psi^{(1)} + \psi^{(2)} + ... + \psi^{(n)}$$

Ou plus explicitement (mais la notation devient alors un peu lourde) :

$$\psi(t, x_1, x_2) = \psi_1^{(1)}(t, x_1) \cdot \psi_2^{(1)}(t, x_2) \; + \; \psi_1^{(2)}(t, x_1) \cdot \psi_2^{(2)}(t, x_2) + ...$$

Dans cette écriture, l'indice du bas correspond à la première ou à la seconde particule et l'indice du haut entre parenthèses est simplement le numéro de la fonction d'onde séparable dans la somme.

Notons que le raisonnement est analogue à ce que l'on avait fait pour l'énergie. Le monde aurait été plus simple si toutes les fonctions d'ondes avaient été séparables (de même qu'il l'aurait été si toutes les particules avaient une énergie bien définie) mais on peut au moins décomposer une fonction d'onde donnée en somme de fonctions séparables pour lesquelles la mécanique quantique reste simple. Ce théorème est en quelque sorte la réciproque de la méthode permettant de construire des états intriqués à partir d'états séparables et précise que tout état intriqué est en fait exactement une somme d'états séparables.

Postulat (Évolution)**.** *Soit une fonction d'onde ψ correspondant éventuellement à un état intriqué. On décompose cette fonction en fonctions d'onde séparables $\psi^{(i)}$. Chaque fonction séparable s'écrit alors comme un produit de deux fonctions d'ondes associées chacune à la position d'une particule. La dynamique de ces fonctions est alors donnée par l'équation de Schrödinger usuelle.*

L'évolution est ainsi quasi la même que pour une particule unique. Comme une fonction d'onde séparable correspond à deux particules «indépendantes», son évolution est

très simple, chaque particule obéit à l'équation de Schrödinger. Pour un état général, on applique ce raisonnement à chaque terme de la somme qui évolue indépendemment des autres. Le fait que l'évolution de la somme soit égale à la somme des évolutions est une conséquence de la linéarité de l'équation de Schrödigner.

Postulat (Mesure)**.** *Les résultats de mesure sont liés à la fonction d'onde de la manière suivante :*

1. Règle de Born : *La (densité de) probabilité de mesurer simultanément la particule 1 en* x_1 et *la particule 2 en* x_2 *à l'instant* t *est donné par le module carré de la fonction d'onde prise en* x_1*,* x_2 *et* t*, i.e. :*

$$Prob(x_1, x_2) = |\psi(t, x_1, x_2)|^2$$

2. Réduction du paquet d'onde : *À l'issue de la mesure, la fonction d'onde est entièrement concentrée sur les deux valeurs* x_1 *et* x_2 *qui ont été mesurées.*

Au sens des probabilités, le module carré de la fonction d'onde fournit ainsi la *loi jointe* des positions des deux particules. La fonction d'onde ne dit pas simplement quelle est la probabilité que telle particule soit à tel endroit, mais aussi la probabilité qu'une particule soit à un certain endroit *sachant* que la seconde particule est à un autre endroit. C'est une information *a priori* beaucoup plus riche que si l'on n'avait qu'une probabilité au niveau de chaque particule, i.e. deux fonctions d'ondes séparées.

En général, on ne veut pas forcément mesurer les deux particules simultanément. Si on ne pouvait faire que ça, la mécanique quantique serait une théorie extrêmement rigide. On peut avoir envie de ne mesurer qu'une seule particule et d'ignorer l'autre ou de mesurer simplement l'une puis l'autre. On aimerait calculer les probabilités dans ces situations et savoir, par exemple, quelle est la fonction d'onde du système composite entre les deux mesures. Il faut pour cela étendre très légèrement le postulat de la mesure. La règle de Born, c'est à dire le passage des fonctions d'onde aux probabilités reste inchangé (notre formulation précédente était déjà assez générale), il faut en revanche légèrement généraliser le postulat de projection du paquet d'onde dans le cas où on ne mesure qu'une seule particule.

Postulat (Mesure partielle)**.** *Les résultats d'une mesure partielle sont liés à la fonction d'onde de la manière suivante :*

1. Règle de Born : *La (densité de) probabilité de mesurer la particule 1 en* x_1 *à l'instant* t *est donnée par la somme des probabilités de mesurer la particule 1 en* x_1 *et la particule 2 en un* x_2 *quelconque.*

$$Prob(x_1) = \underset{\{tous\ les\ x_2\}}{Somme}\ Prob(t, x_1, x_2) = \int_{x_2=-\infty}^{x_2=+\infty} |\psi(t, x_1, x_2)|^2\, dx_2$$

2. Réduction du paquet d'onde : *À l'issue de la mesure, la fonction d'onde est concentrée uniquement sur la valeur* X_1 *qui vient d'être mesurée, i.e. :*

$$\begin{aligned} \psi(t, x_1, x_2) &\propto \psi(t, X_1, x_2)\ si\ x_1 = X_1 \\ &= 0\ si\ x_1 \neq X_1 \end{aligned}$$

Le signe «$\propto$*» signifie «proportionnel à», il peut en effet être nécessaire de multiplier ce résultat par une constante pour garantir que la somme des probabilités vaille toujours 1.*

Le premier point de ce postulat est simplement une conséquence de ce que sont les probabilités. La probabilité de mesurer la première particule à un endroit est égale à la probabilité de mesurer la première particule à cet endroit et la seconde n'importe ou, il n'y a pas grand chose de surprenant. La seconde partie du postulat précise que toute la fonction d'onde ne collapse pas lors d'une mesure partielle, en fait on ne collapse que selon la position qui vient d'être mesurée ce qui est finalement compréhensible : on n'a extrait d'information que sur cette coordonnée. Attention d'ailleurs à ne pas confondre ici x_1 qui est une variable de la fonction d'onde, qui reste *a priori* libre même après la mesure et X_1 qui est la position effectivement mesurée qui est une constante après la mesure.

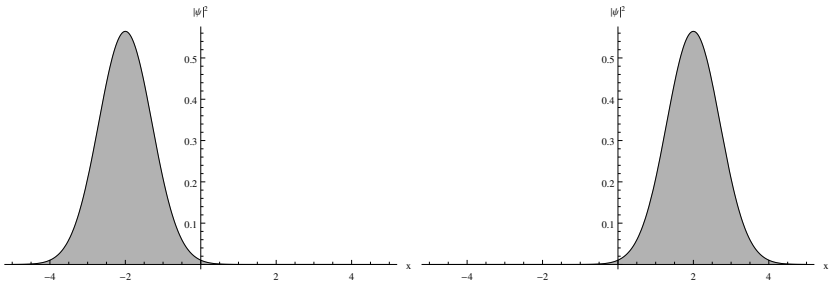

FIGURE 1 – ψ_g et ψ_d

.2 L'intrication

Jusqu'à maintenant tout a pu paraître très formel. Le problème est qu'il est difficile de parler d'intrication précisément sans avoir introduit ce qui précède car c'est un concept qui défie assez fortement l'intuition.

La première question que l'on peut se poser maintenant que l'on a donné le formalisme est de savoir comment représenter la fonction d'onde d'un état composite. Si on a un état séparable, alors la fonction d'onde totale est le produit de deux fonctions d'onde que l'on peut traiter séparément. Dans ce cas la situation est très simple, il suffit de représenter les deux fonctions d'onde séparément. Pour rendre les choses plus claires ou au moins explicites, introduisons deux fonctions d'onde typiques qui vont nous être utiles par la suite. On va pour le moment oublier le temps et ne considérer que des fonctions d'onde statiques [9]. On va supposer que l'espace est borné (typiquement que l'on est dans une boîte) et considérer deux fonctions d'onde (à une particule) particulières, l'une concentrée à gauche ψ_g, et l'autre concentrée à droite ψ_d (voir Fig. 1). L'état séparable $\psi_{gd}(x_1, x_2) = \psi_g(x_1)\psi_d(x_2)$ est simplement l'état où la première particule est à droite et la seconde particule est à gauche. De la même manière on peut définir l'état $\psi_{dg}(x_1, x_2) = \psi_d(x_1)\psi_g(x_2)$ qui est l'état où les positions sont inversées. L'interprétation de ces deux états séparables est, on le voit, relativement simple. On peut désormais considérer un état intriqué pour se rendre compte que la situation est un peu plus complexe. Considérons par exemple l'état [10] $\psi_{EPR} = \psi_{gd} + \psi_{dg}$ (voir Fig. 2). Dans ce cas, l'état du système composite est une superposition d'un état où la particule 1 est à gauche et la particule 2 à droite et d'un état où la particule 1 est à droite et la particule 2 à gauche. On voit bien qu'il est impossible d'attribuer dans ce cas à chaque particule une fonction d'onde indépendante : l'état du système est complètement intriqué (au sens quantique comme au sens usuel du terme). On a indicé des lettres «EPR» cet état intriqué particulier pour «Einstein-Podoslky-Rosen» du nom des physiciens qui ont étudié un état de ce type en 1935 pour mettre en évidence certaines difficultés conceptuelles de la mécanique quantique.

Si l'on mesure la première particule à gauche, alors on est certain qu'à l'issue de la mesure, la seconde particule est forcément à droite et inversement, si on mesure la première particule à droite on sait que la seconde est alors à gauche : on peut connaître les propriétés de la deuxième particule en mesurant seulement la première, leurs deux destins sont liés. Il faut noter que cela reste évidemment vrai si les deux particules sont dans des boîtes différentes éventuellement très éloignées (par exemple dans deux galaxies différente). L'intrication quantique peut lier les propriétés des particules sur des distances arbitrairement grandes. C'est ce que l'on a à l'esprit quand on dit que la mécanique quantique est intrinsèquement non locale.

9. On peut par exemple imaginer que les fonctions d'onde que l'on considère ont une énergie bien définie et donc que leur module carré n'évolue pas. Alternativement, on peut simplement considérer que l'on fait l'expérience vite devant le temps caractéristique de la dynamique imposée par l'équation de Schrödinger.

10. Une fois encore cet état est défini à une normalisation près. Il faudrait en toute rigueur multiplier ψ_{EPR} par $1/\sqrt{2}$ pour que l'égalité soit correcte. Comme le raisonnement est ici un peu heuristique, on peut oublier les constantes multiplicatives.

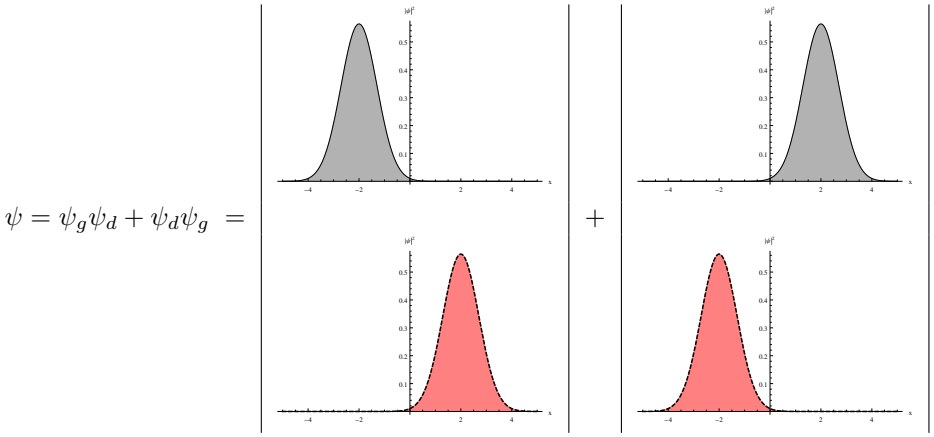

FIGURE 2 – Représentation de la fonction d'onde d'un état intriqué

.3 Discrétisation

Avant de poursuivre on peut introduire une notation qui va subrepticement rattacher le formalisme de la fonction d'onde que l'on utilise actuellement à celui plus abstrait des états discrets. L'objectif est ici d'introduire la notation de Dirac que l'on rencontre constamment dans la littérature sur la mécanique quantique (et dont les signes cabalistiques peuvent rebuter le lecteur) sans pour autant introduire le formalisme mathématique un peu lourd des espaces de Hilbert.

On aime bien, en mécanique quantique, considérer des systèmes ayant un nombre fini d'états possibles (chat mort ou vivant, particule à gauche ou à droite, particule ayant une énergie E_1 ou une énergie E_2) plutôt que la position elle même qui possède un continuum de valeurs possibles. C'est finalement ce que l'on a fait sans le dire dans le paragraphe précédent en ne considérant plus que deux fonctions d'onde ψ_g et ψ_d, c'est à dire des fonctions d'onde correspondant à une particule à gauche ou à droite, au lieu de toutes les fonctions d'onde possibles. En se restreignant à ces deux possibilités, on a en quelque sorte discrétisé la position en refusant volontairement de s'intéresser à ses détails. Si on considère une boîte constituée de deux compartiments «gauche» et «droit», cela revient à ne plus s'intéresser qu'au compartiment dans lequel se trouve la particule et plus à sa position à l'intérieur d'un compartiment. Dans ce cas, on peut oublier la forme précise de la fonction d'onde dans chaque compartiment et ne plus retenir qu'une donnée binaire, gauche ou droite, pour l'état de la particule. On utilise alors généralement une notation due à Dirac dont l'utilité n'est malheureusement pas évidente dans ce contexte (mais qui est utile pour comprendre la littérature) et on écrit $\psi_g = |g\rangle$ et $\psi_d = |d\rangle$. Un état écrit sous la forme $|\cdot\rangle$ s'appelle alors un *ket*[11]. On n'écrit plus explicitement l'argument x de la fonction, c'est à dire la position, parce qu'elle est contenue dans le «gauche» ou «droite». L'état EPR se réécrit alors de la manière compacte suivante (voir aussi Fig. 3) :

$$|\psi_{EPR}\rangle = |g\rangle|d\rangle + |d\rangle|g\rangle$$

Ce que l'on lit parfois, l'état EPR est une superposition de l'état gauche-droite (particule 1 à gauche, particule 2 à droite) et de l'état droite-gauche. On introduit parfois la mécanique quantique en partant de ce formalisme et en écrivant l'état du système sous la forme d'une somme de *kets* à l'intérieur desquels on inscrit les propriétés du système. On peut par exemple considérer l'état de trois particules (quantiques) que l'on peut disposer dans 5 boites et donner au hasard un état intriqué du système :

$$|\psi\rangle = |\text{"boite 2"}\rangle|\text{"boite 1"}\rangle|\text{"boite 3"}\rangle + |\text{"boite 1"}\rangle|\text{"boite 4"}\rangle|\text{"boite 5"}\rangle$$

11. Comprendre l'origine de ce nom n'est pas très évident à ce stade. Il faut en fait introduire un autre objet noté $\langle\cdot|$ que l'on appelle alors un «*bra*». Quand on fait agir le second sur le premier on obtient l'analogue d'un produit scalaire de vecteurs que l'on note alors $\langle\cdot|\cdot\rangle$ (lire «braket»). Un ket est donc simplement la moitié d'un braket (en français on pourrait dire qu'un «chet» est la moitié d'un crochet.)

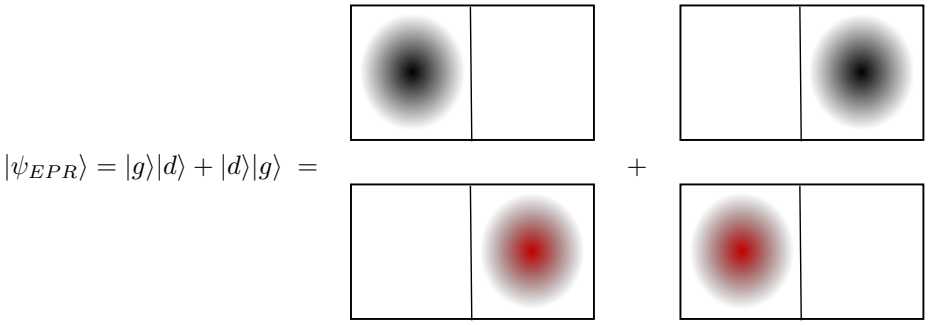

FIGURE 3 – Représentation de la fonction d'onde d'un état intriqué

Cet état est un état intriqué (ou superposé) somme d'un état (ou d'une situation) où la particule 1 est dans la boite 2, la 2 dans la 1 et la 3 dans la 3 et d'un état où on a 1 dans 1, 2 dans 4 et 3 dans 5. Cette notation est largement utilisée car elle est assez commode et on oublie ainsi vite les fonctions d'onde des particules. Il faut cependant se souvenir que ce sont bien elles qui donnent un sens à cette formule et qui précisent ce que signifient cette somme et cette fameuse «superposition quantique». Se souvenir que cette notation fait référence, in fine, aux fonctions d'onde (et aux postulats auxquelles ces dernières obéissent) est la seule manière de comprendre *vraiment* ce qu'elle signifie (au moins d'un point de vue opérationnel). Par extension, on a tendance à généraliser cette notation à des propriétés qui ne sont pas liées de manière directe à la position comme «atome excité» ou «atome désexcité» ou même :

$$|\text{chat \& atome}\rangle = |\text{mort}\rangle|\text{atome désexcité}\rangle + |\text{vivant}\rangle|\text{atome excité}\rangle$$