Société de Calcul Mathématique SA
Outils d'aide à la décision
depuis 1995

Informatique Quantique :

Analyse critique de l'état de l'art

Rapport adressé au

Service du Numérique,

Secrétariat Général des Ministères Economiques et Financiers

par la

Société de Calcul Mathématique SA

Version finale, octobre 2023

Le présent rapport est établi en application de la commande du 28/08/2023, numéro d'engagement 1512110078, service FAC9470075, Service du numérique, Secrétariat Général des Ministères Economiques et Financiers.

Résumé opérationnel

Ce rapport est divisé en deux parties :

1. **Cryptographie**

La préoccupation à l'origine de cette étude est simple à décrire : l'informatique quantique (en abrégé IQ) est-elle susceptible de mettre en danger les algorithmes usuels de cryptographie ?

Ceux-ci, en effet, reposent sur la constatation suivante : étant donné un grand nombre entier N, produit de deux nombres premiers : $N = n_1 \times n_2$, il est très difficile de trouver les facteurs n_1, n_2 si on ne connaît que le produit N. L'algorithme de cryptographie le plus utilisé est RSA-2048: le nombre N a 2048 chiffres en écriture binaire, soit 617 chiffres en écriture décimale ; il est inviolé à ce jour.

L'Informatique Quantique permettrait d'accélérer de beaucoup la recherche des facteurs, mettant ainsi en danger la sécurité du cryptage. La question qui nous est posée est : cette affirmation est-elle crédible ?

La "National Academy of Sciences", USA, dans son rapport "Quantum Computing: Progress and Prospects (2019)" apporte un premier élément de réponse :

Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade.

La NAS a consulté des spécialistes du sujet, qui n'ont pas voulu aller trop vigoureusement contre les annonces de toute la profession et de toute la presse. Notre réponse sera beaucoup plus précise et beaucoup plus simple :

L'utilisation de l'IQ pour casser un code de cryptographie relève de la mystification ; les algorithmes présentés sont purement académiques et ignorent les principes fondamentaux de la mécanique quantique.

Détaillons nos arguments :

1. La mécanique quantique repose sur un formalisme mathématique (dû à Von Neumann) qui est une simplification de la réalité ; ce formalisme échoue à décrire correctement les expériences modernes (fentes d'Young et intrication). On ne peut espérer construire une machine (en l'occurrence un ordinateur quantique) à partir d'une description de la réalité aussi insatisfaisante.

2. Le principe de l'Informatique Quantique repose sur l'intrication : réalisation d'une fonction d'onde globale, incorporant tous les systèmes partiels. On travaillerait d'un seul coup sur cette fonction globale, d'où une accélération des calculs. Mais Erwin Schrödinger dit clairement que, dans le cas de systèmes intriqués, la connaissance de la fonction d'onde globale,

pour l'ensemble du système, ne donne pas une connaissance parfaite des fonctions d'onde de chacun des sous-systèmes : l'information se dilue. Les auteurs d'algorithmes d'IQ, qui apparemment n'ont jamais lu Schrödinger, font comme si, à chaque instant, ils conservaient la connaissance de tous les sous-systèmes. Leur travail est un travail "idéal", purement académique, qui méconnaît les règles fondamentales de la mécanique quantique.

3. La mécanique quantique étant fondamentalement probabiliste, il est exclu que, N étant donné, elle puisse produire de façon déterministe les facteurs n_1, n_2 : tout au plus pourra-t-elle produire des résultats avec une certaine probabilité : celle-ci est inconnue.

Nous ajouterons deux arguments qui, à notre avis, sont moins significatifs :

4. Un ordinateur quantique requiert des conditions de travail très particulières : température au voisinage du zéro absolu, pas de bruit, pas de vibrations, et temps de calcul très court (quelques nano-secondes). Cela rend la réalisation concrète très difficile à l'heure actuelle, mais il n'est pas impossible que les limitations technologiques soient levées dans l'avenir.

5. Un article récent de Jin-Yi Cai (University of Wisconsin-Madison), juin 2023, s'intitule : *Shor's Algorithm Does Not Factor Large Integers in the Presence of Noise*. L'algorithme de Shor est considéré comme le plus prometteur pour casser les procédés de cryptographie. Mais Jin-Yi Cai fait lui-même une hypothèse académique sur la nature du "bruit" qui viendrait perturber le signal principal, c'est-à-dire la fonction d'onde du système intriqué. En réalité, personne ne sait à quoi peut ressembler cette fonction d'onde.

Nous rejoindrons complètement la National Academy of Sciences :

Key Finding 6: Quantum computing is valuable for driving foundational research that will help advance humanity's understanding of the universe. As with all foundational scientific research, discoveries from this field could lead to transformative new knowledge and applications.

Notre conclusion à cette première partie sera :

Les algorithmes de cryptographie ne sont pas menacés, mais on a tout à gagner à poursuivre la recherche en Informatique Quantique, à commencer par une meilleure compréhension des phénomènes physiques. Dans l'histoire de l'humanité, beaucoup de découvertes ont été faites "ad augusta per angusta", et la recherche de la pierre philosophale a précédé de beaucoup l'établissement de la chimie moderne.

2. Paradoxes de la Mécanique Quantique

Dans une seconde partie, comme demandé par le Service du Numérique, nous élargissons la réflexion : elle ne concerne plus la cryptographie, mais traite, plus généralement, des paradoxes de la Mécanique Quantique : existence ou non de variables cachées et explications apportées par les inégalités de Bell.

Nous procédons à l'analyse critique d'un article de D. Marchand : "Le paradoxe EPR et l'inégalité de Bell", disponible en ligne (cours de l'École supérieure de physique et de chimie industrielles

de la ville de Paris). Il se consacre à l'analyse de l'intrication et est divisé en deux parties. La première décrit une analogie physique simple : un canon à clous. Malheureusement, l'auteur prouve alors qu'il ignore les lois fondamentales des probabilités. Dans la seconde, l'auteur applique le raisonnement à l'intrication de deux photons et, à ce moment, il prouve qu'il ignore également les lois fondamentales de la mécanique quantique.

Nous donnons les prescriptions nécessaires pour que l'expérience des photons ait une valeur quantitative et sorte du mysticisme. Enfin, nous concluons en nous référant à la position prise par Albert Einstein : il existe une explication assez simple au fait que deux photons intriqués manifestent des polarisations proches, en cas de mesure, même s'ils sont séparés par de grandes distances.

Introduction

Le présent rapport est établi en application de la commande du 28/08/2023, numéro d'engagement 1512110078, service FAC9470075, Service du numérique, Secrétariat Général des Ministères Economiques et Financiers.

Il nous est agréable de remercier ce Service pour un thème d'étude particulièrement original et intéressant.

Réserves de propriété : il n'y en a pas. Le présent travail représente une analyse critique publique de données, travaux, informations, qui sont eux-mêmes publics. Il peut être diffusé sans restriction.

Table des matières

Première Partie

Informatique Quantique

et

Cryptographie

I. Notre analyse

Nous commençons par la mise en évidence de deux points essentiels, qui ne sont mentionnés par aucun spécialiste du sujet, à une exception près (voir plus bas) :

- L'ensemble de la mécanique quantique repose sur un formalisme mathématique (dû à Von Neumann) qui est artificiel, empirique, et dont la validité réelle est inconnue ;

- Ce formalisme commence par introduire un concept fondamental, qui est celui de fonction d'onde. L'idée de base de l'informatique quantique est que plusieurs systèmes élémentaires peuvent être "intriqués" (voir plus bas), c'est-à-dire représentés par une fonction d'onde unique, sur laquelle on pourra faire tous les calculs.

Mais Erwin Schrödinger, dans son livre "Physique quantique et représentation du monde" dit clairement que, dans le cas de systèmes intriqués (il emploie le mot "entremêlement", mais nous gardons la terminologie moderne), la connaissance de la fonction d'onde globale, pour l'ensemble du système, ne donne pas une connaissance parfaite des fonctions d'onde de chacun des sous-systèmes : l'information se dilue. Dans le cas qui nous occupe ici, nous avons affaire à un très grand nombre de sous-systèmes et les auteurs font comme si chacun d'eux restait parfaitement connu après intrication.

Autrement dit, même si on accepte le formalisme de Von Neumann, la connaissance précise des éléments après intrication est loin d'être aussi précise que le voudraient les auteurs des algorithmes.

A. Validité d'un formalisme

Le formalisme intrinsèque de la mécanique quantique repose sur l'utilisation des espaces de Hilbert : situation très particulière, où l'on dispose d'un produit scalaire et d'une distance euclidienne ; il est essentiellement dû à Von Neumann dans les années 1950 et n'a jamais été remis en cause depuis. Le concept principal est celui d'un opérateur dans un espace de Hilbert et on admet que, après mesure, les valeurs propres de l'opérateur jouent un rôle essentiel.

Or ce formalisme n'a aucune justification physique : il n'y a rien qui permette de croire que la Nature se laisse décrire par un formalisme hilbertien. C'est un choix commode (le formalisme hilbertien est simple à manipuler), consensuel, mais entièrement arbitraire.

Dire par exemple que la probabilité de trouver une particule au voisinage d'une position donnée, à un instant donné, est proportionnelle au carré du module de la fonction d'onde évaluée à cet endroit à cet instant (énoncé fondamental de la mécanique quantique) est consensuel, mais entièrement dépourvu de justification.

Il en résulte ceci, qui sera très important pour la suite : toute conclusion obtenue par déduction logique à partir du formalisme mathématique de la mécanique quantique est à prendre avec beaucoup de prudence. Un article très récent de Jin-Yi Cai [Cai], juin 2023, dit la même chose.

Cette conclusion est vraie, à des degrés divers, pour la plupart des lois physiques et de leur interprétation mathématique. Pour bien comprendre ceci, prenons l'exemple très simple et très connu de la loi de l'attraction universelle, de Newton : $F = k\frac{mm'}{d^2}$; elle est certainement juste en général, mais :

– Elle est évidemment fausse à très courte distance ;

– On ne comprend pas comment la force peut se propager ;

– Elle ne permet pas de répondre à des questions simples, telle la stabilité du système solaire ;

– Elle est incompatible avec la théorie de la relativité.

Cela ne signifie évidemment pas qu'il faille renoncer à la loi de Newton : il faut simplement se souvenir qu'elle a des limites. C'est pire encore avec la mécanique quantique, parce que les fondements sont beaucoup plus récents et beaucoup moins satisfaisants sur le plan conceptuel. Il est légitime de dire que le formalisme actuel est approprié à l'investigation (il permet de poser les questions), mais qu'il ne doit pas être considéré comme fournissant des réponses fiables et encore moins la construction d'appareils ayant une réalité physique.

Il ne faut surtout pas critiquer Von Neumann pour avoir introduit ce formalisme : pour lui, il avait une valeur préliminaire, permettant d'établir des lois qui seraient ensuite confrontées à l'expérience. A aucun moment Von Neumann n'a prétendu avoir "découvert" les lois mathématiques régissant la mécanique quantique.

B. Le recours à l'expérience

La seule méthode pour améliorer une loi conceptuelle est de la tester par comparaison avec ce que donne l'expérience. Or, en mécanique quantique :

– Les expériences sont très difficiles à réaliser ;
– Les experts sont en désaccord fondamental sur l'interprétation des résultats.

Comme nous allons le voir, des expériences de plus en plus nombreuses et de mieux en mieux contrôlées mettent en évidence des faits qui sont rationnellement incompréhensibles. Aucune explication rationnelle n'existe à ce stade et les tentatives d'explication sont contradictoires.

C. Des faits bien étayés, totalement incompréhensibles

3. La dualité onde-corpuscule

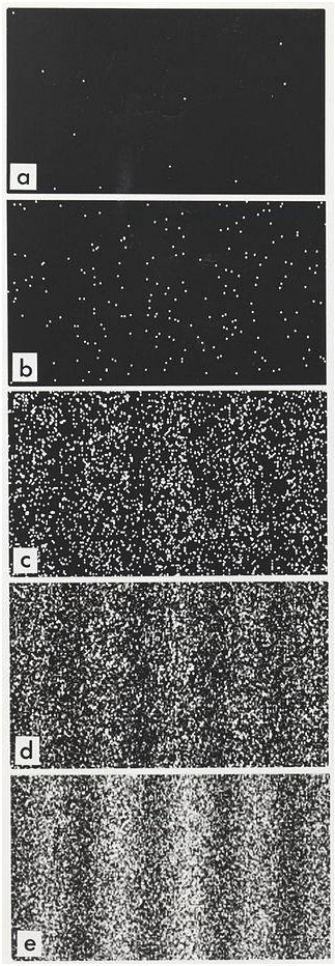
Elle repose sur une expérience faite de multiples fois et bien décrite : celle des "fentes d'Young" (1801). Si on envoie un faisceau d'électrons au travers de deux trous, apparaissent des interférences sur un écran situé au-delà des trous. Les experts sont en désaccord sur l'interprétation.

Il y a une incohérence fondamentale dans les explications qui sont données :

On nous dit en effet :

Si on lance un petit nombre d'électrons, un par un, ils se répartissent uniformément sur l'écran (figure 1 ci-dessous ; voir https://fr.wikipedia.org/wiki/Fentes_de_Young).

Des franges d'interférence apparaissent seulement lorsqu'on lance un grand nombre d'électrons.



L'interprétation quantique du phénomène est la suivante : le quantum émis prend un état superposé lors du franchissement de la plaque : |quantum passe par S1〉 + | quantum passe par S2〉 . De la fonction d'onde résultante, on peut déterminer pour chaque point de la plaque la probabilité que le quantum y soit détecté. On peut démontrer que la distribution des probabilités suit la figure d'interférence. Autrement dit, le quantum passerait par les deux fentes à la fois, et interférerait avec lui-même".
https://fr.wikipedia.org/wiki/Fentes_de_Young

Mais alors le phénomène doit se manifester pour chaque électron pris individuellement, et pas seulement si le nombre est élevé.

Dans les expériences modernes, on sait émettre les électrons successivement et de manière indépendante : le $n^{ème}$ est déjà arrivé sur l'écran lorsque le $n+1^{ème}$ est émis : il n'est donc pas possible que chaque électron puisse interférer avec les précédents ou les suivants. Comme la présence de franges est un fait d'expérience, on en conclut qu'elle se produit même dans le cas d'un seul électron (mais en ce cas on ne voit pas les franges) ; chaque électron emprunte les deux trous et interfère avec lui-même.

Dans l'expérience la plus récente [Bach], on explique que la distance entre les deux fentes est 0.3×10^{-6} m, tandis que la taille d'un électron est de l'ordre de 10^{-22} m (elle n'est pas connue exactement). Il y a là une bizarrerie qui n'est pas relevée par les auteurs. Nous sommes tout à fait disposés à admettre que l'on ne connaît pas la position exacte de l'électron (on ne peut parler que de "probabilité de présence" dans un secteur donné), mais cela ne permet pas à un objet tout petit d'être en deux endroits distincts à la fois. La manière dont les électrons sont lancés n'est pas claire dans la publication : on parle de "canon à électrons".

Retenons ce qui paraît indiscutable, après lecture de cette publication, qui est bien faite.

– Il y a effectivement des franges d'interférence, même dans le cas d'un seul électron ;

– Si on bouche l'une des fentes, les franges disparaissent.

La conclusion nécessaire est que l'électron est plus gros qu'on ne le croit : il ne se limite pas à une toute petite corpuscule, de taille 10^{-22} m, mais inclut nécessairement un "support physique" plus gros. Que ce support prenne la forme d'une onde, c'est très possible.

De toute évidence, quelque chose appartenant à l'électron passe par chacune des deux fentes ; il ne faut pas tomber dans le mysticisme et affirmer qu'une toute petite corpuscule peut se trouver à deux endroits à la fois.

Une remarque nécessaire est la suivante : lorsqu'on lit les présentations faites par les spécialistes, un sur deux affirme "les objets sont dans plusieurs états à la fois" et un sur deux "tout objet ne peut être que dans un seul état à la fois". Il y a complète incohérence entre les explications qui sont fournies.

On peut certainement admettre (voir plus haut) que l'électron ait une probabilité de présence dans plusieurs endroits séparés ; on peut à la rigueur admettre que l'électron soit en fait un "gros" objet, dont une partie passera par une fente et l'autre partie passera par l'autre fente. Mais si on s'intéresse aux vitesses (ce qui est parfaitement légitime en mécanique quantique), il devient difficile d'admettre que l'électron va à la fois à 1000 km/s et à 2000 km/s. En ce cas, il n'y aurait plus de séparation temporelle : une partie de l'électron serait déjà arrivée alors qu'une partie n'a pas encore démarré. L'électron serait "lié" à ses positions passées et futures, ce qui est incompréhensible pour nous.

4. L'intrication

Elle est encore plus difficile à comprendre que la dualité onde-corpuscule. L'expérience montre que, dans certaines conditions, des électrons ou des photons qui ont été "intriqués" à un moment donné continuent à interagir, même lorsqu'ils sont séparés, et ce quelle que soit la distance qui les sépare. Concrètement, une mesure faite sur l'un d'entre eux (et qui donc révélera l'état du premier) aura pour effet de révéler aussi l'état du second, instantanément. Les expériences mettant cet effet en évidence sont maintenant nombreuses ; la plus spectaculaire porte sur des photons émis par un satellite et recueillis dans deux laboratoires distants de 1 300 km [Yin].

Il n'existe pour le moment aucune explication à ce phénomène ; une description dans le formalisme de la mécanique quantique consiste à dire que le système formé par les deux particules a une unique fonction d'onde (quelle que soit la distance) et que par conséquent toute mesure, sur l'un ou sur l'autre, altère cette fonction d'onde, ce qui se manifeste par un choix déterministe sur l'autre particule. Mais ceci n'est qu'un formalisme, qui n'explique absolument rien. Comment expliquer que deux particules très éloignées aient une fonction d'onde commune, superposition de leurs fonctions d'onde élémentaires ?

L'intrication pourrait se manifester non seulement dans l'espace, mais aussi dans le temps : une étude de l'Université Hébraïque de Jérusalem de 2013 [Megidish] montre que deux photons n'ayant jamais coexisté pouvaient être intriqués. On commence par deux photons intriqués et on envoie l'un d'eux sur une autre paire, totalement distincte, et des corrélations apparaissent.

Les limites de ces expériences ne sont absolument pas claires ; elles ont l'immense mérite de montrer qu'il existe un phénomène qui échappe à la logique usuelle. Mais dans quelles conditions ? Quelles particules sont susceptibles d'intrication ? Quelles sont les conditions expérimentales ? Combien de temps dure l'intrication, et quelles sont les perturbations possibles ? Dans le cas de la réception par deux laboratoires distants de 1 300 km, à partir d'un même satellite, quelle est la proportion de paires qui ont manifesté une intrication ?

Est-ce un phénomène permanent et constant, ou bien se manifeste-t-il seulement pour certaines paires, dans certaines conditions ?

5. Les réserves formulées par Erwin Schrödinger

Dans son livre "Physique quantique et représentation du monde", Schrödinger étudie explicitement la fonction d'onde résultant d'un système intriqué. Et il écrit (page 119 de l'édition française) : *"La meilleure connaissance possible d'un ensemble [donnée par la fonction d'onde du système complet] n'inclut pas nécessairement la meilleure connaissance possible de chacune de ses parties […]. L'état du système est donné par la fonction d'onde ψ, qui est la somme maximale des connaissances relatives au système entier. L'ensemble est dans un état déterminé, mais ce n'est pas le cas de chacune des parties prises séparément".*

Page 120 : *"Initialement, le catalogue commun des prévisions [pour les sous-systèmes] est formé de la somme logique des catalogues individuels ; durant le processus, il évolue nécessairement en suivant une loi connue [l'équation de Schrödinger] (et jusqu'ici il n'est pas question de mesure). Notre savoir demeure maximal, mais à la fin, lorsque les deux corps [intriqués] se séparent à nouveau, il ne se compose plus de la somme logique des savoirs relatifs à chacun d'entre eux. Ce qui en est alors conservé peut être devenu très inférieur à ce maximum. On remarque qu'il y a une très grande différence avec la théorie classique des modèles dans laquelle, naturellement, la connaissance des états initiaux et de l'interaction permet de déterminer les états finaux."*

Dans une note page 169, note 102, Michel Bitbol précise ceci de manière très claire : "*En mécanique quantique, la connaissance des états initiaux et de l'interaction permet de déterminer l'état final du système global, mais pas les états finaux des sous-systèmes qui le constituent*.".

6. Des conditions de fonctionnement très strictes et peu claires

Il semble que l'intrication (de photons, d'électrons) ne puisse être réalisée que dans des conditions expérimentales extrêmement strictes : il faut une température proche du zéro absolu, le noir complet, aucune influence extérieure d'aucune sorte (pas de vibrations, etc.) et que, malgré tout, le phénomène ait une durée de vie extrêmement brève (personne ne sait pourquoi). Dans la plupart des publications, les conditions de fonctionnement ne sont décrites que de manière très vague. En particulier, le taux d'échec n'est jamais mentionné.

D. L'ordinateur quantique

1. Le hardware

Du point de vue du hardware : c'est un cryostat, c'est-à-dire une chambre froide, fonctionnant à température proche du zéro Kelvin : 15 milli-Kelvin. Pour obtenir un tel résultat, on utilise de l'hélium superfluide pour le refroidissement.

L'information peut être portée, selon les technologies mises en œuvre :

- par des "ions piégés", qui peuvent être excités ou non ;
- par des supraconducteurs, qui peuvent être dans deux états.

Le principe adopté par IBM, Google, et d'autres consiste à encoder chaque Qubit sous la forme d'un minuscule circuit de supraconducteurs. Pour que les ordinateurs quantiques délivrent une prestation optimale, les Qubits doivent conserver leur état quantique intact jusqu'à la fin du calcul.

Il existe beaucoup d'autres tentatives technologiques, que nous n'aborderons pas ici : notre approche concerne les fondements théoriques.

2. La représentation de l'information par Qubits

On dispose par exemple d'un photon, dont la polarisation peut être verticale ou horizontale, ou la superposition des deux. A partir de là, en se servant des nombres complexes, on peut définir un point dans l'espace réel de dimension 3, appelé "sphère de Bloch" (il s'agit d'une sphère à cause de la normalisation : voir plus bas).

On note $|0\rangle, |1\rangle$ ces deux états et un état quantique quelconque s'écrit sous la forme d'une combinaison linéaire à coefficients complexes :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

avec la normalisation :

$$|\alpha|^2 + |\beta|^2 = 1 \qquad (2)$$

On peut toujours supposer que α est réel positif. On dispose en théorie de 4 degrés de liberté dans (1), qui se réduisent à 2, puisque α est réel positif et du fait de la normalisation (2).

On associe à ψ un point de $\mathbb{R}^3$ grâce aux coordonnées sphériques :

$$x = \sin(\vartheta)\cos(\varphi), y = \sin(\vartheta)\sin(\varphi), z = \cos(\vartheta)$$

où ϑ, φ sont des angles définis par :

$$\alpha = \cos\left(\frac{\vartheta}{2}\right),\ 0 \le \vartheta \le \pi\ ;\ \beta = e^{i\varphi}\sin\left(\frac{\vartheta}{2}\right),\ 0 \le \varphi < 2\pi.$$

ψ est la fonction d'onde ; $|\alpha|^2$ est la probabilité de mesurer le Qubit sur $|0\rangle$ (polarisation verticale) et $|\beta|^2$ est la probabilité de mesurer le Qubit sur $|1\rangle$ (polarisation horizontale). La somme fait évidemment 1.

Selon Maxime Dion, Institut Quantique, Université de Sherbrooke, Canada, il est possible de fabriquer des photons intriqués en utilisant un cristal biréfringent. Voir :
https://www.usherbrooke.ca/iq/ressources/curieux-quantiques/reflexions-quantiques/voir-double-grace-a-lintrication/

Si on dispose de deux Qubits, on écrira :

$$c_1 |00> + c_2 |01> + c_3 |10> + c_4 |11>$$

où les nombres c_1, c_2, c_3, c_4 sont ceux que l'on veut stocker, et la notation $|00>, |01>$, *etc.*, représente une base hilbertienne permettant de stocker cette information ; on pourrait aussi bien la représenter sous la forme des quatre suites $(0,0),(0,1),(1,0),(1,1)$. Comme les nombres sont complexes, on a en principe 8 degrés de liberté, mais on en perd 2 : c_1 peut être pris réel positif et on a la normalisation $\sum_{i=1}^{4} |c_i|^2 = 1$.

Si on dispose de n Qubits, on aura pour base les 2^n suites constituées de 0 et de 1 et on pourra stocker 2^n informations (en fait $2^n - 2$ pour les raisons vues précédemment).

L'informatique quantique prétend ainsi sa supériorité sur l'informatique ordinaire, qui, sur n bits, ne pourra stocker que n informations.

3. Une antériorité risible

Pour un mathématicien professionnel, cette prétention à l'antériorité a quelque chose de risible. Nous savons depuis longtemps utiliser des bases hilbertiennes pour représenter l'information ; la plus connue est celle des exponentielles complexes e^{int}, où n est un entier relatif quelconque (positif ou négatif) ; elle est constamment utilisée en transformation de Fourier (depuis 1820), en particulier pour le traitement du signal. Bien d'autres bases sont utilisées : le système de Walsh, le système de Haar, du nom de leurs créateurs (voir notre livre [Beauzamy] pour plus de précisions). Il est complètement évident, depuis au moins 200 ans, qu'en choisissant convenablement une base on peut représenter une quantité importante d'information sur cette base, et la récupérer facilement si la base est orthogonale.

Prenons un exemple simple pour illustrer ceci :
La fonction :

$$f(x) = \frac{\cos(x)}{2} + \sqrt{2}\cos(x)^2 - \frac{4\cos(x)^3}{5} + \frac{1}{2}\mathrm{i}\sin(x) + 2\mathrm{i}\sqrt{2}\cos(x)\sin(x) - \frac{12}{5}\mathrm{i}\cos(x)^2\sin(x) - \sqrt{2}\sin(x)^2 + \frac{12}{5}\cos(x)\sin(x)^2 + \frac{4}{5}\mathrm{i}\sin(x)^3$$

paraît très compliquée. Or c'est seulement :

$$f(x) = \frac{\mathrm{e}^{\mathrm{i}x}}{2} + \sqrt{2}\mathrm{e}^{2\mathrm{i}x} - \frac{4}{5}\mathrm{e}^{3\mathrm{i}x}$$

Par conséquent, si on s'est mis d'accord sur le fait qu'on utilisait la base des exponentielles complexes, pour transmettre f il suffit de transmettre les trois nombres $\left(1/2, \sqrt{2}, -4/5\right)$.

Un autre exemple est encore plus simple : si on s'est mis d'accord sur un livre de référence, il suffira de transmettre "p12, ligne45" pour désigner une phrase.

4. Obstacles à la réalisation d'un ordinateur quantique

Nous reprenons ici la présentation de la conférence [Bobroff].

Les principaux défis sont les suivants :

- Fabriquer des bits quantiques ;
- Les intriquer ;
- Les garder en vie assez longtemps pour pouvoir faire les calculs (temps : de l'ordre de 100 microsecondes) ;
- Faire des portes logiques pour manipuler les données ;
- Savoir écrire un programme.

Pour le premier, il faut par définition construire un système qui puisse prendre deux états ; comme dit plus haut, il y a à l'heure actuelle deux solutions technologiques en concurrence :

- Systèmes à base d'ions piégés, qui peuvent être excités ou non ;
- Systèmes à base de supraconducteurs : ce sont des circuits électriques pouvant prendre deux états.

L'intrication ne peut être réalisée que dans des conditions physiques très particulières : très basse température, aucun bruit d'aucune sorte. Il n'existe dans la littérature aucune information sur le taux de réussite de l'opération : quand on essaie d'intriquer deux électrons, ou deux photons, y parvient-on à chaque fois ? de temps en temps ? une fois sur dix mille ?

La durée de vie de l'intrication paraît extrêmement faible (nous l'avons dit plus haut : de l'ordre de 100 microsecondes, soit 10^{-4} s). Dans la conférence [Bobroff], on apprend qu'un satellite situé à 500 km d'altitude a envoyé des photons intriqués à deux villes chinoises distantes de 1 200 km (on ne connaît pas la position du satellite par rapport à chacune des villes).

Admettons un parcours de 500 km à la vitesse de la lumière (300 000 km/s), cela nous donne un temps de parcours de 1.67×10^{-3} s, ce qui est très supérieur au temps maximal annoncé pour l'intrication. La présentation dit "il y a une paire sur un million qui marche" : on ne comprend pas le sens de cette assertion. Selon l'article de référence [Yin et al.], le satellite émet de l'ordre de 5.9 millions de paires de photons intriquées par seconde ; chaque paire est ensuite dirigée sur une ville ou sur l'autre. La théorie quantique dit ceci : je mesure le jumeau A, qui peut

prendre les valeurs 0 ou 1 ; disons que je trouve 0 ; alors nécessairement le jumeau B est dans l'état 1, ce que confirmera la mesure de B.

Mais, si la théorie quantique est vérifiée, ceci devrait se produire pour toutes les paires, et pas seulement pour une fraction d'entre elles. En effet, sur le plan des probabilités élémentaires, lorsque j'émets d'innombrables paires de photons (A, B), il est fréquent que la mesure de A et la mesure de B donnent des résultats opposés.

5. Les "Erreurs" dans le calcul quantique

Il est très difficile de comprendre ce que ce terme recouvre exactement. Dans la conférence [Bobroff], l'auteur prend l'exemple de l'extraction d'un prénom dans une liste (voir plus bas) ; on peut admettre dans ce cas qu'une erreur se traduit par le fait que le prénom résultant du traitement n'est pas le bon. L'erreur ne peut être définie que par référence à un but, complètement déterministe, qui n'est pas atteint.

Mais la mécanique quantique étant essentiellement probabiliste, il ne peut y avoir d'erreur dans la manipulation des concepts : la mesure d'une grandeur donne différents résultats avec différentes probabilités ; ce n'est pas une erreur.

La conférence [Bobroff] mentionne un taux d'erreur d'environ un pour mille opérations, du fait de l'environnement et du bruit. Pour un ordinateur normal, l'estimation est d'une erreur sur 10^{20} opérations.

Une difficulté supplémentaire tient au fait que, dans le cas quantique, on n'a pas le droit d'arrêter le calcul pour vérifier les étapes intermédiaires. En cas d'arrêt intermédiaire, tout s'effondre. Pour remédier à cette difficulté, l'approche la plus utilisée consiste à cloner le système, c'est-à-dire à mettre en place plusieurs systèmes identiques, sur lesquels on fait les mêmes calculs ; avec un taux d'erreur de 1/1000 (actuellement), il faut 10 000 jumeaux par Qubit. Pour 100 Qubits utiles, il en faut donc un million de Qubits mobilisables. En pratique, on sait fabriquer à l'heure actuelle des ordinateurs quantiques avec environ 60 Qubits : on est loin du compte.

6. Un exemple concret : trouver un prénom dans une liste

La conférence [Bobroff] prend cet exemple : trouver un prénom dans une liste de 1 000, sachant qu'il y a un prénom par page du livre. Nous donnons plus loin (voir Annexe I) une analyse technique détaillée de l'article auquel cet exemple se réfère.

Très grossièrement, l'approche retenue est de la forme suivante :

- On réalise une "superposition" des prénoms : on obtient une fonction d'onde qui est la superposition de toutes les fonctions individuelles ;
- On compare cette fonction d'onde à celle relative au prénom "Julien" ;
- On accentue la "bosse" de la fonction d'onde relative au prénom "Julien" ;

– On réitère jusqu'à ce que cette bosse devienne significative.

Cette procédure, de nature probabiliste, ne donne pas toujours la bonne réponse : il faut recommencer. On mesure seulement à la fin, lorsqu'on estime que la fonction d'onde est suffisamment éloquente.

Nous émettons des réserves quant à la validité de cet article :

– Il prétend que l'informatique traditionnelle ne sait pas résoudre ce problème rapidement. Or cela dépend de la manière dont les données sont présentées et ce temps de présentation disparaît de l'analyse en ce qui concerne l'approche quantique. En d'autres termes, on suppose que les données sont mal présentées si elles doivent être traitées par un ordinateur classique, bien présentées si elles le sont par un ordinateur quantique.

– La description mathématique de l'algorithme n'est pas convaincante et nous estimons qu'elle recèle des erreurs de logique.

– Enfin, et surtout, elle néglige la réserve fondamentale formulée par Erwin Schrödinger et exposée au début du présent rapport : lorsqu'on fabrique la fonction d'onde, superposition des fonctions d'onde individuelles, l'information élémentaire est très largement perdue et rien ne dit qu'on saura retrouver un prénom particulier au milieu des autres.

Annexe 1

Analyse critique de l'article

Quantum Mechanics helps in searching for a needle in a haystack
Lov K. Grover
Phys.Rev.Lett.79:325-328,1997

Cet article sert de base à la conférence de Julien Bobroff.

1. Présentation du besoin

Il s'agit de trouver un nom dans une liste de N noms, arrangée en ordre quelconque.

L'article prétend que l'informatique quantique permet de le faire en $O\left(\sqrt{N}\right)$ opérations et que l'informatique ordinaire ne peut le faire qu'en $O(N)$ opérations.

La notation $O(\ )$, dite "notation de Landau", signifie "proportionnel à", sans qu'on connaisse le coefficient de proportionnalité ; un nombre d'opérations en $\frac{N}{2}$ et $10\,000\,N$ seront tous deux notés $O(N)$.

2. Préparation de la liste

La présentation de l'article est fallacieuse depuis le début. En réalité, tout dépend de la manière dont la liste a été préparée, et cette préparation doit être incluse dans le temps d'exécution.

Dire que l'informatique traditionnelle requiert en moyenne $\frac{N}{2}$ opérations se réfère à la situation où l'on tourne l'une après l'autre les pages d'un livre, où l'on veut découvrir le prénom attendu ("Julien", dans la conférence de M. Bobroff). Effectivement, si le livre a 1 000 pages, en moyenne l'exploration se terminera à 500. Mais si la liste a été préalablement arrangée par ordre alphabétique, on peut aller beaucoup plus vite : on commence par consulter la page 500 et voir si elle est avant ou après "Julien". Si elle est avant, c'est que Julien se trouve entre 500 et 1 000 ; si elle est après, c'est que Julien se trouve entre 1 et 500 et on répète par dichotomie. Le nombre de manipulations est alors $Log(N)$.

En outre, Microsoft dispose de structures extrêmement efficaces (appelées "dictionnaires") pour retrouver un nom dans une liste.

Venons-en maintenant à l'article lui-même.

3. Difficultés techniques

On dispose d'un système pouvant prendre $N = 2^n$ états, correspondant à une suite $x_1,...,x_n$ où chaque x_i peut valoir ± 1. On numérote $\nu = 1,...,N$ ces états et on les note S_ν. On suppose que l'un de ces états est intéressant et on veut le retrouver dans la liste des N. L'article parle d'une "fonction d'évaluation", $C(S_\nu)$, qui retourne 1 si l'état est celui qui nous intéresse, 0 sinon.

Par exemple, si $n = 4,\ N = 2^4 = 16,$ les états sont de la forme $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ où tous les ε valent ± 1. On peut décider par exemple que la situation d'intérêt est $(1,-1,1,1)$ et il faut retrouver ce quadruplet parmi les 16 possibles.

L'article utilise un principe de superposition en mécanique quantique. Initialement, tous les $N-uplets$ S ont la même probabilité, c'est-à-dire la même fonction d'onde, mais à chaque étape l'analyse de $C(S)$ (qui vaut 1 ou 0, suivant que S est la suite recherchée ou non) conduit à une modification de cette fonction d'onde : celle correspondant au "bon" S se trouve renforcée et les autres se trouvent diminuées, si bien qu'au bout d'un certain nombre de répétitions, le bon S va avoir une probabilité très proche de 1, et c'est à ce moment-là qu'on fait la mesure (n'oublions pas que, en mécanique quantique, la mesure réduit la fonction d'onde). L'article prétend (nous ne discuterons pas ce point) que l'évaluation de chaque $C(S)$ n'est pas une mesure et donc ne perturbe pas les fonctions d'onde.

L'approche de l'article est la suivante :

On énumère les $S_\nu, \nu = 1,...,N.$ Si $C(S) = 1,$ on fait un changement de phase dans la fonction d'onde, si $C(S) = 0,$ on ne fait rien. On applique ensuite au système une matrice (purement déterministe) qui aura pour effet d'accentuer les changements. L'article prétend qu'il suffit de répéter cette opération $\sqrt{N}$ fois pour que la probabilité du bon S s'accroisse.

Or, il n'y a qu'un seul bon S parmi N. On peut réaliser les tests séquentiellement ($\nu = 1,2,...$), cela ne change rien au problème. Lorsqu'on a fait $\sqrt{N}$ tests, il y a $N - \sqrt{N}$ items qui n'ont pas été testés, et le bon peut parfaitement se trouver parmi ceux-là. Plus précisément, la probabilité que le bon se trouve parmi les testés est $\frac{\sqrt{N}}{N}$ et la probabilité qu'il se trouve parmi les non-testés est $\frac{N - \sqrt{N}}{N},$ qui est évidemment beaucoup plus grand.

Disons les choses simplement : si nous faisons seulement $\sqrt{N}$ tests, il y a toute chance pour que ces tests portent exclusivement sur les S mauvais : le bon ne sera pas détecté. Et dans ces conditions, le traitement ultérieur que fait l'article (application d'une matrice déterministe) ne portera que sur l'affaiblissement des $\sqrt{N}$ détectés comme mauvais et ne permettra en rien l'identification du bon, qui reste noyé dans les $N - \sqrt{N}$ restants.

Un autre aspect que l'article n'aborde absolument pas est celui du nombre d'opérations nécessaires à la préparation des données. Pour l'informatique traditionnelle, nous l'avons vu plus haut, on se place dans le pire cas.

Mais ici, prenons la situation $1024 = 2^{10}$; comment associer une liste de 1024 prénoms à une liste de 1024 pages, sous la forme d'une liste $(\varepsilon_1,...,\varepsilon_{10})$, où chaque $\varepsilon = \pm 1$? A priori, le lien logique n'est pas clair : il y a $1024!$ ordres possibles pour l'ensemble des prénoms dans les pages du livre. Si la question est "il y a un unique Julien et il faut savoir à quelle page il est", on pensera à mettre $\varepsilon_k = 1$ si Julien est en page k, -1 sinon. Mais alors toutes les suites d'intérêt seront faites de 9 fois -1 et une seule fois $+1$; il y a seulement 10 suites de ce type et toute la discussion précédente est sans intérêt.

4. Objection fondamentale

L'objection de Erwin Schrödinger est de nature fondamentale : lorsque nous constituons la fonction d'onde du système intriqué (constitué des 1 000 prénoms), nous perdons l'information spécifique relative à chaque prénom. Dès lors, comment être sûr du bon fonctionnement du mécanisme $C(S)$, qui vaut 1 ou 0, suivant que S est la suite recherchée ou non, à partir de la fonction d'onde globale ?

Annexe II

L'algorithme de Shor

Peter W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, 1994.
Voir https://fr.wikipedia.org/wiki/Algorithme_de_Shor

Les systèmes usuels de cryptographie (RSA) reposent sur la donnée d'un très grand nombre, dont il est impossible en théorie de connaître les facteurs premiers. Le nombre peut ainsi être rendu public.

Soit $N = pq$ où p, q sont premiers.

On considère, pour x entier, la suite $x \bmod N, x^2 \bmod N, x^3 \bmod N, etc.$, où $\bmod N$ désigne le reste après division par N. On montre que si x n'est divisible ni par p, ni par q, cette suite se répète avec une période qui est un diviseur de $(p-1)(q-1)$.

En répétant ceci pour diverses valeurs de x, on en déduit la valeur de $(p-1)(q-1)$, puis les valeurs de p et q séparément.

Mais, même si la séquence $x \bmod N, x^2 \bmod N, x^3 \bmod N, etc.$, se répète, le nombre d'étapes pourrait être presque aussi grand que N lui-même (qui peut avoir des milliers de chiffres).

La partie quantique de l'algorithme de Shor vise à créer une superposition de tous les nombres de la suite $x \bmod N, x^2 \bmod N, x^3 \bmod N, etc.$ Une fois cette superposition faite, on en déduit la période de la suite ; on répète ceci pour un nombre suffisant de valeurs de x et on peut espérer en déduire les diviseurs de N.

La contribution "quantique" se limite au fait que certains calculs peuvent être faits en une seule fois, alors que l'approche traditionnelle exige des calculs séquentiels. Mais ceci n'est possible que si on sait réaliser la fonction d'onde du système intriqué constitué par la superposition de tous les nombres de la suite $x \bmod N, x^2 \bmod N, x^3 \bmod N, etc.$

L'objection fondamentale de Erwin Schrödinger est a fortiori valable ici.

Un article récent de Jin-Yi Cai (University of Wisconsin-Madison), juin 2023, s'intitule :
Shor's Algorithm Does Not Factor Large Integers in the Presence of Noise

Il dit en résumé :

"We consider Shor's quantum factoring algorithm in the setting of noisy quantum gates. Under a generic model of random noise for (controlled) rotation gates, we prove that the algorithm does not factor integers of the form pq when the noise exceeds a vanishingly small level in terms of n — the number of bits of the integer to be factored, where p and q are from a well-defined set of

primes of positive density. We further prove that with probability 1 − o(1) over random prime pairs (p, q), Shor's factoring algorithm does not factor numbers of the form pq, with the same level of random noise present."

Autrement dit, même en faisant des hypothèses académiques sur la nature des erreurs qui vont se rencontrer, l'algorithme ne fonctionnera pas. Ceci, bien entendu, se rajoute à l'objection fondamentale de Schrödinger.

L'article dit aussi ceci, qui rejoint bien les objections fondamentales que nous avons mentionnées au début de ce rapport :

"It has often been pointed out that the availability of these quantum gates at high precision (with arbitrarily small angles in R_k *with* $k \to \infty$*) is a challenge, both intellectually and practically on engineering grounds. To a large extent, such concerns motivated another great intellectual achievement that is the development of quantum error correcting codes. There is a substantial body of work on fault tolerant quantum computing, starting with Shor's work. Strong threshold theorems are proved which show that in certain error models, if the error rate is below a certain threshold, quantum computation can achieve arbitrarily high accuracy. These are beautiful mathematical theorems.* ***But they fundamentally assume that the group SU(2) exactly corresponds to operations on a qubit in reality, especially in its composition—that group composition (in its infinite precision defined over C) exactly corresponds to sequential application of realizable quantum operations. Opinions differ, as to whether such arbitrary precision is ever achievable. It is certainly a possibility. However, this author is skeptical about this, based on the belief that quantum mechanics itself (just as any other physical theory) is not, and is not meant to be, infinitely accurate when comparing reality with what the mathematical statements say in the theory (some speculations are in Section 4).*** *Meanwhile, enormous efforts have been underway in the past few decades, and with much renewed momentum and enthusiasm more recently, to achieve ever increasingly accurate hardware implementations of quantum circuitry."*

Annexe III

Les conclusions de la National Academy of Sciences, USA

Quantum Computing: Progress and Prospects (2019)
http://nap.nationalacademies.org/25196

La conclusion suivante répond bien aux interrogations des utilisateurs de cryptographie :

Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade. (Chapter 7).

Mais nous ne sommes pas d'accord avec l'approche retenue par la NAS, qui repose sur la consultation d'experts internes à la discipline ; la conclusion du rapport est :

Based on evaluation of publicly available information regarding progress to date in the field of quantum computing, the committee saw no fundamental reason why a large, fault-tolerant quantum computer could not be built in principle.

Notre conclusion est beaucoup plus pessimiste :

- On ne comprend rien au formalisme de la mécanique quantique ;
- Même en admettant ce formalisme, l'objection fondamentale de Schrödinger montre que les calculs précis sont impossibles ;
- On ne comprend rien aux expériences qui sont faites (dont la plupart ont une validité expérimentale indiscutable : les expériences sont bien faites) ;
- Dans ces conditions, imaginer qu'on saura réaliser un appareil sachant effectuer des calculs précis relève de l'imagination.

Références

[Bach] Roger Bach et al 2013 New J. Phys. 15 033018.

[Beauzamy] Bernard Beauzamy : Introduction to Banach Spaces and their Geometry. North Holland, Collection "Notas de Matematica", vol. 68. Première édition : 1982, seconde édition : 1985.

[Bobroff] Julien Bobroff, conférence faite à l'Institut d'Astrophysique de Paris, 12/03/2020 : https://youtu.be/cNoiw6jMCz4

[Cai] Jin-Yi Cai : Shor's Algorithm Does Not Factor Large Integers in the Presence of Noise https://doi.org/10.48550/arXiv.2306.10072, juin 2023.

[Dion] Maxime Dion, Institut Quantique, Université de Sherbrooke, Canada : https://www.usherbrooke.ca/iq/ressources/curieux-quantiques/reflexions-quantiques/voir-double-grace-a-lintrication/

[Grover] Lov K. Grover: Quantum Mechanics helps in searching for a needle in a haystack, 1997 https://doi.org/10.48550/arXiv.quant-ph/9706033

[Megidish] E. Megidish, A. Halevy, T. Shacham, T. Dvir, L. Dovrat, and H. S. Eisenberg Entanglement Swapping between Photons that have Never Coexisted Phys. Rev. Lett. 110, 210403 – Published 22 May 2013

[Von Neumann] Les fondements mathématiques de la Mécanique quantique, 1946.

[Schrödinger] Physique quantique et représentation du monde, coll. "Points-Sciences". Le Seuil, 1992 (ISBN 2-02-013319-9).

[Yin] Juan Yin et al. : Satellite-based entanglement distribution over 1200 kilometers, 2017 https://www.science.org/doi/10.1126/science.aan3211

Seconde Partie

Mécanique quantique, variables cachées et inégalités de Bell

Résumé Opérationnel de la Seconde Partie

Le débat est très vif, depuis des dizaines d'années, à propos des explications possibles d'expériences relatives à l'"intrication" réalisées dans le cadre de la mécanique quantique : deux particules, ayant été en contact à un moment donné, partageraient ensuite des caractéristiques communes, quelle que soit la distance qui les sépare.

Ce qui rend difficile toute compréhension du sujet, c'est d'abord que les spécialistes se contredisent. Par exemple, sur la dualité onde-corpuscule, pour expliquer les fentes d'Young, la moitié des experts affirme que les particules se trouvent dans plusieurs endroits à la fois, tandis que l'autre moitié soutient, avec la même ardeur, que chaque particule se trouve dans un seul endroit.

Pour tenter d'y voir clair, nous procédons à l'analyse critique de l'article de D. Marchand : "Le "paradoxe" EPR et l'inégalité de Bell", qui est en ligne (cours de l'École supérieure de physique et de chimie industrielles de la ville de Paris) :
https://cours.espci.fr/site.php?id=200&fileid=752

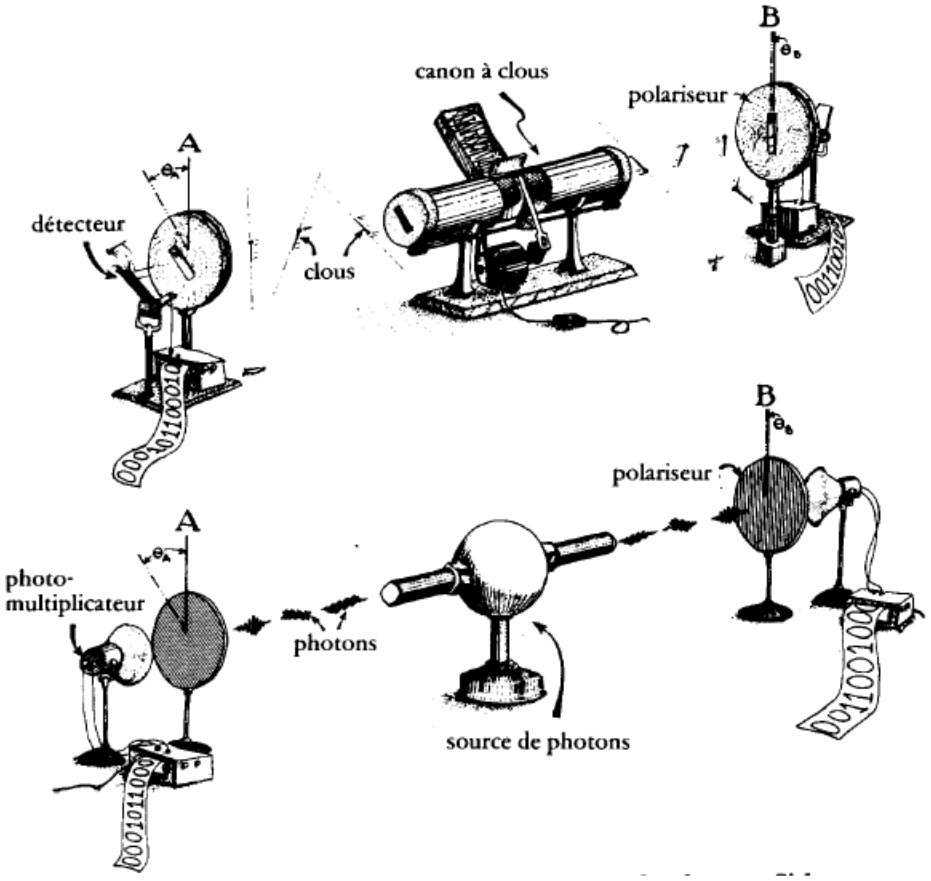
Cet article se consacre à l'analyse de l'intrication ; il est divisé en deux parties. La première décrit une analogie physique simple : un canon à clous. Malheureusement, l'auteur prouve alors qu'il ignore les lois fondamentales des probabilités. Dans la seconde, l'auteur applique le raisonnement à l'intrication de deux photons et, à ce moment, il prouve qu'il ignore également les lois fondamentales de la mécanique quantique. Même en physique atomique, deux ignorances ne font pas une science.

Nous donnons les prescriptions nécessaires pour que l'expérience des photons ait une valeur quantitative et sorte du mysticisme : il faut connaître la loi de probabilité régissant la différence de polarisation (contrairement à ce qui est dit, les deux photons émis simultanément n'ont pas de raison d'avoir exactement la même polarisation) et il faut connaître exactement la tolérance du dispositif : la fente ayant une orientation donnée, quelle tolérance sur l'orientation du photon est acceptable pour qu'il passe par la fente ?

Enfin, nous concluons en nous référant à la position prise par Albert Einstein : il existe une explication assez simple au fait que deux photons intriqués manifestent des polarisations proches, en cas de mesure, même s'ils sont séparés par de grandes distances.

I. Premier Chapitre : le canon à clous

Le dessin ci-dessous est extrait de cet article.



Le texte qui suit est extrait de l'article ; nous mettons nos commentaires entre crochets : à ce stade, ils concernent des rectifications de vocabulaire. Notre analyse complète est donnée plus loin, dans un paragraphe séparé.

A. Extrait de l'article

Imaginons un canon à clous, qui tire simultanément deux clous dans deux directions opposées. Imaginons qu'au lieu de partir pointe en avant, les clous qui sortent du canon aient leur tige perpendiculaire à l'axe de tir. Nous supposerons de plus que deux clous d'une même paire ont leurs tiges parallèles [*rectification : de même orientation*], mais les différentes paires possèdent des orientations parfaitement aléatoires les unes par rapport aux autres. On mitraille deux plaques de métal, A et B, percées chacune d'une fente. Ces fentes se comportent comme de véritables polariseurs parce qu'elles ne laissent passer que les clous dont l'orientation est parallèle [*identique*] à la leur et arrêtent tous les autres. Nous supposerons qu'il est possible de modifier l'orientation des polariseurs au cours de l'expérience. On place près des plaques deux observateurs qui comptent les clous passant ou ne passant pas la fente. Le passage d'un clou est marqué par un 1, le non-passage par un 0.

Au début, les deux polariseurs sont orientés dans la même direction. Comme les deux clous d'une même paire ont exactement la même orientation et que les polariseurs A et B sont alignés, chacun des clous ou bien passe par la fente ou bien « rate son coup ». Les succès et les échecs sont en parfaite corrélation en A et B [*mal dit : il ne s'agit pas de corrélation ; simplement, la liste des résultats est identique pour A et pour B*] :

Par exemple :

A : 0100011001000010110100110010110001000100
B : 0100011001000010110100110010110001000100

Chaque séquence de 0 et de 1 est aléatoire parce que le canon tire chaque paire dans toutes les directions [*mal dit : les paires sont toutes dans des plans perpendiculaires à l'axe des récepteurs, mais les orientations dans ces plans sont aléatoires*]. Remarquons que ces deux séquences aléatoires sont exactement corrélées [*identiques*].

A présent, modifions l'angle relatif des deux polariseurs en faisant pivoter dans le sens des aiguilles d'une montre la fente de la plaque A ; elle forme alors un angle θ avec la fente de la plaque B. Avec une telle géométrie, il est possible qu'un clou d'une paire passe par la fente A et que l'autre rate la fente B, ou l'inverse. De plus, comme les fentes sont assez larges, il est encore possible que les deux clous passent en A et B. Les succès et les échecs en A et B ne seront plus exactement corrélés [*les listes ne seront plus identiques*]. L'enregistrement des résultats aura alors une allure du genre :

A : 0001011000101011100011110010110010100100
B : 0011001000101011100011010010010010100100

Dans l'article, on indique par une flèche les "erreurs" de corrélation. Le nom d'"erreurs" convient parce qu'on peut considérer qu'il s'agit d'erreurs dans le résultat de A par rapport à celui de B, que nous prendrons comme référence *[le mot "erreur" ne convient pas du tout : il s'agit simplement de différences entre A et B].*

Dans l'exemple ci-dessus, il y a 4 erreurs sur 40 tirs, de sorte que le taux d'erreur E (θ) est égal à 10%.

Supposons maintenant que nous ne touchions pas au polariseur A et que nous fassions pivoter le polariseur B d'un angle θ, mais cette fois-ci dans le sens contraire des aiguilles d'une montre. Nous pouvons dire que les erreurs se trouvent dans le résultat obtenu en B, par rapport à A pris comme référence. Le taux d'erreur sera le même que précédemment, E (θ) =10%, puisque la géométrie est la même.

Enfin, faisons tourner le polariseur A d'un angle θ dans le sens des aiguilles d'une montre et le polariseur B également d'un angle θ, mais dans le sens contraire. L'angle relatif des deux polariseurs est maintenant de 2θ. Quel est le taux d'erreurs dans cette configuration ? Il est facile de répondre à cette question si nous supposons que les erreurs en A sont indépendantes de ce qui se passe en B, et vice-versa. Ce faisant, nous faisons l'hypothèse de causalité locale. Après tout, il n'y a aucune raison pour que la situation en B ait un quelconque effet sur le passage du

clou dans la fente A. Puisque les erreurs en B étaient précédemment de E (θ), nous devons leur ajouter les erreurs provoquées par la rotation du polariseur A, c'est-à-dire, là encore, E(θ). Il semble donc que le nouveau taux d'erreur doive être égal à la somme des deux taux d'erreur mutuellement exclusifs, soit E(θ) + E(θ) = 2E(θ).

[Commentaire SCM : ceci est totalement absurde. Les deux clous d'une même paire sont, au lancement, exactement dans la même orientation. L'angle entre les deux polariseurs étant connu, le passage en A et en B sont liés de manière totalement déterministe : voir calcul plus bas.]

Mais attention : en faisant pivoter A d'un petit angle θ, nous avons perdu ce qui nous servait de référence pour le résultat enregistré en B ; de même, en faisant pivoter B, nous avons perdu ce qui nous servait de référence pour le résultat en A. Cela signifie que, lorsque de temps en temps, se produira une double erreur – c'est-à-dire une erreur à la fois en A et B - cette double erreur sera enregistrée comme "pas d'erreur". Par exemple, supposons qu'une paire de clous donne les résultats 1 en A et 1 en B lorsque les polariseurs sont parfaitement alignés. Si le polariseur A est légèrement tourné, le clou rate la fente et l'observateur note 0. On a donc une erreur de corrélation [*non : une différence dans les résultats*]. Mais puisque le polariseur en B a également été tourné, il est possible que le clou arrivant en B manque aussi la fente. On a alors affaire à une double erreur, au cours de laquelle deux 1 (1 en A et 1 en B) ont été transformés en deux zéros (0 en A et 0 en B). Comme ces deux zéros ne produisent aucune erreur de corrélation, la double erreur passe inaperçue, si bien que le taux d'erreur pour un angle 2θ entre les polariseurs, E (2θ), est nécessairement inférieur à la somme des taux d'erreurs enregistrés précédemment de façon séparée. C'est ce qu'exprime mathématiquement la formule :

$$E(2\theta) \leq 2E(\theta)$$

qui porte le nom d'inégalité de Bell.

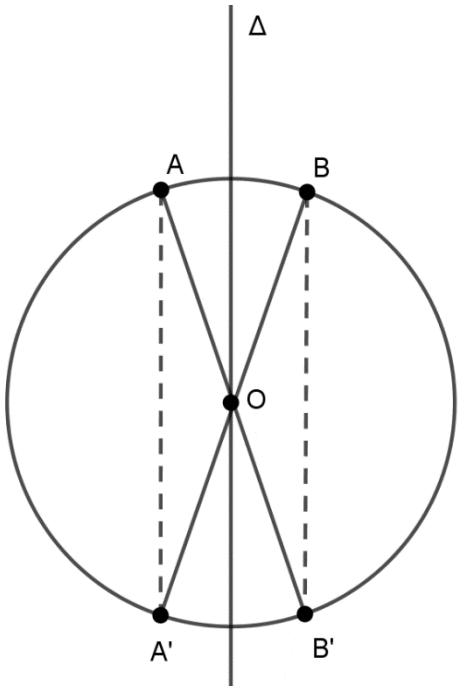
B. La description de la SCM

La description faite plus haut est fondamentalement incorrecte, essentiellement du fait d'un vocabulaire inapproprié.

Faisons une description précise du dispositif.

Le canon à clous est situé à l'origine ; il tire vers les $x<0$ et vers les $x>0$. Les deux récepteurs sont situés respectivement en $x=-1$ et $x=1$. Les paires de clous sont émises simultanément et les deux clous, dans chaque paire, ont la même orientation. Celle-ci est définie par un "segment" de longueur 1, situé dans le plan vertical perpendiculaire à Ox. L'orientation du segment est définie par un angle φ, angle avec l'horizontale : l'équation du support est donc de la forme $z=y\tan(\varphi)$ et l'angle φ suit une loi uniforme entre 0 et 2π ; l'orientation des segments est donc aléatoire, suivant une loi uniforme : aucune direction n'est privilégiée. Mathématiquement parlant, un segment est représenté par un diamètre d'un cercle : les milieux de tous les segments sont à l'origine, les segments sont d'épaisseur nulle et on ne distingue pas entre les deux extrémités (elles ne sont pas peintes de couleurs différentes).

Un récepteur comporte une fente, selon le modèle suivant :



La fente est constituée de l'ensemble $AOBA'OB'$; en réalité, la partie hachurée ne sert à rien. Un clou qui arrive est un segment dont le milieu est en O ; il passera si et seulement si son extrémité supérieure est entre A et B (et donc son extrémité inférieure entre A' et B').

Notons φ_1 l'angle du segment avec la verticale (donc $\varphi_1 = \varphi - \frac{\pi}{2}$, puisque φ est l'angle avec l'horizontale) et ε l'angle $(OA, \Delta) = (\Delta, OB)$; la largeur de la fente est donc 2ε.

La condition nécessaire et suffisante pour que le segment passe dans la fente est donc $|\varphi_1| < \varepsilon,$ ou encore :

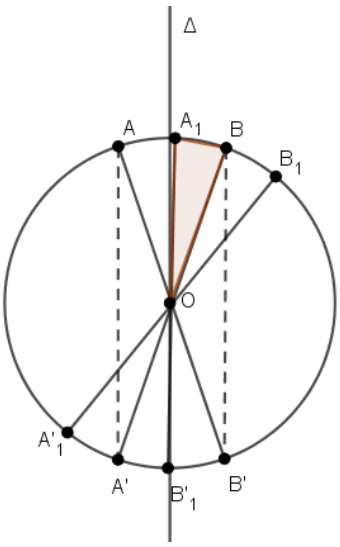
$$\frac{\pi}{2} - \varepsilon < \varphi < \frac{\pi}{2} + \varepsilon.$$

Il s'agit toujours d'inégalités strictes : le segment ne peut pas frotter sur les bords de la fente. Celle-ci est entièrement caractérisée par l'arc de cercle AB et son symétrique $A'B'$.

La proportion de segments qui passent dans la fente, pour chaque récepteur, est donc $p = \frac{4\varepsilon}{2\pi} = \frac{2\varepsilon}{\pi}$ (un segment peut arriver la tête en bas). Cette proportion est évidemment indépendante de l'orientation du récepteur, puisque l'émetteur émet uniformément dans toutes les directions.

Considérons maintenant ce qui se passe au second récepteur. Celui-ci a une fente de même forme, mais l'axe de la fente fait un angle ϑ avec la verticale (on peut évidemment supposer que la fente du premier récepteur est verticale).

Contrairement à ce que dit l'article, le sort du second segment est entièrement connu à partir du sort du premier. Le second segment a le même angle avec la verticale, donc on peut calculer facilement l'angle qu'il fait avec l'axe de la seconde fente, puisque l'angle ϑ des axes des deux fentes est connu.



Dans le dessin ci-contre, les deux fentes ont été superposées ; la fente AOB tourne d'un angle de 20° et devient A_1OB_1 ; on comprend très bien ce qui arrive : le premier segment passe s'il est entre A et B et le second s'il est entre A_1 et B_1. Comme les deux segments ont la même orientation, cela revient à regarder la figure constituée d'une superposition des deux fentes et un seul segment.

– On aura succès conjoint (les deux segments passeront) si le segment unique est entre A_1 et B (intersection des deux fentes) ;
– On aura échec conjoint si le segment unique est en dehors de AB_1 (réunion des deux fentes) ;

– On aura succès de l'un et échec de l'autre, et donc différence de résultat, si le segment unique est entre A et A_1 ou entre B et B_1. Les probabilités de chaque cas sont faciles à calculer.

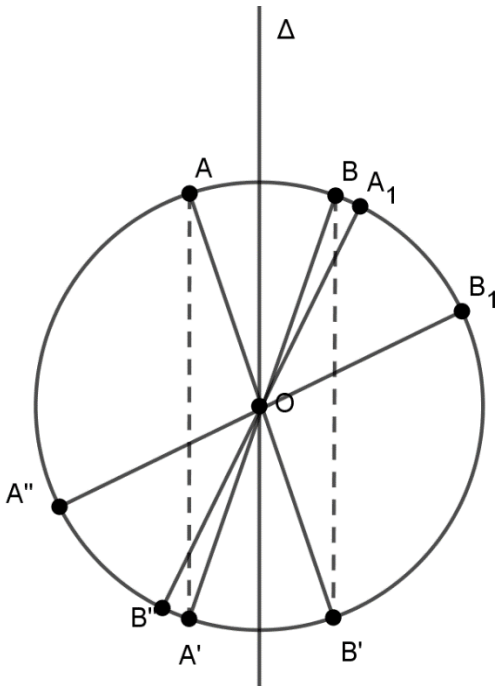
Cas 1 : les deux fentes ont une partie commune

La première s'étend sur $\left]\frac{\pi}{2}-\varepsilon,\frac{\pi}{2}+\varepsilon\right[$, la seconde sur $\left]\frac{\pi}{2}-\varepsilon-\vartheta,\frac{\pi}{2}+\varepsilon-\vartheta\right[$; il y aura recouvrement si $\frac{\pi}{2}-\varepsilon<\frac{\pi}{2}+\varepsilon-\vartheta$, soit $\vartheta<2\varepsilon$. L'arc BA_1 s'étend de $\frac{\pi}{2}-\varepsilon$ à $\frac{\pi}{2}+\varepsilon-\vartheta$; il a donc pour longueur $2\varepsilon-\vartheta$. L'arc AA_1 s'étend de $\frac{\pi}{2}+\varepsilon$ à $\frac{\pi}{2}+\varepsilon-\vartheta$: il a pour longueur ϑ, et de même pour l'arc BB_1.

La probabilité d'une différence (appelée succès de l'un et échec de l'autre) est donc $p_d=\frac{4\vartheta}{2\pi}=\frac{2\vartheta}{\pi}$ si $\vartheta<2\varepsilon$, c'est-à-dire tant que A_1 reste entre A et B.

Cas 2 : les deux fentes n'ont plus de partie commune

Si A_1 est à droite de B, les deux fentes n'ont plus de partie commune.



Si le segment tombe entre A et B, ou entre A_1 et B_1, il passera pour l'un des récepteurs et non pour l'autre ; la probabilité est $p_d = \frac{8\varepsilon}{2\pi} = \frac{4\varepsilon}{\pi}$ qui est indépendant de ϑ.

Nous avons donc obtenu :

Proposition. – *Notons ε la demi-largeur de la fente (angle de tolérance) et ϑ l'angle de rotation entre les deux capteurs. La probabilité d'une différence de résultat entre les bâtons lancés à gauche et à droite est :*

$p_d(\vartheta) = \frac{2\vartheta}{\pi}$ si $\vartheta < 2\varepsilon$;

$p_d(\vartheta) = \frac{4\varepsilon}{\pi}$ si $\vartheta \geq 2\varepsilon$.

Il est donc évident que $p_d(2\vartheta) \leq 2p_d(\vartheta)$, mais pas du tout pour les raisons mentionnées dans l'article. En particulier, il n'y a aucune indépendance entre les comportements aux deux capteurs.

II. Second Chapitre : le canon à photons

Nous retournons maintenant à la lecture de l'article, seconde partie.

A. Lecture de l'article

Ces deux hypothèses – **objectivité** et **causalité locale** – sont essentielles à la démonstration de l'inégalité de Bell. Que se passe-t-il si maintenant nous remplaçons les clous par des photons ?

Au lieu d'un canon à clous, nous allons utiliser comme source de particules des positroniums. Un positronium est un "atome" constitué d'un seul électron lié à un positron (ou anti-électron) ; cet atome se décompose, de façon totalement aléatoire, en deux photons émis dans des directions opposées, et (c'est là le point crucial), dont les polarisations relatives sont exactement corrélées [*identiques*]- tout comme celles des clous. La désintégration du positronium est telle que si l'un des photons a une polarisation le long d'une certaine direction, l'autre photon, celui qui part dans la direction opposée, a la même polarisation. La direction absolue de la polarisation des deux photons change de manière aléatoire d'une désintégration à l'autre, mais leur polarisation relative reste la même. C'est là une caractéristique importante de la source – qui fait qu'elle ressemble au canon à clous.

Les photons partent dans des directions opposées et passent au travers de polariseurs très éloignés l'un de l'autre, placés en *A* et *B*. Quant aux observateurs, ce sont des tubes photomultiplicateurs placés derrière chacun des polariseurs et capables de détecter des photons uniques. Si un photomultiplicateur détecte un photon, l'événement est signalé par un 1 ; si

aucun photon n'est détecté, l'appareil marque un 0. Dans la configuration initiale, les deux polariseurs A et B sont parfaitement alignés l'un par rapport à l'autre. Faisons en sorte que le polariseur B soit fixe et que A puisse tourner sur lui-même ; soit ϑ l'angle relatif des deux polariseurs. Dans la configuration initiale, donc, $\vartheta = 0.$

Si un photon touche le polariseur, il a une certaine probabilité de passer à travers et d'être détecté. Si un photon a une polarisation parallèle à la direction de passage du polariseur, il parvient jusqu'au détecteur et on enregistre un 1. Si la polarisation du photon est perpendiculaire à la direction du polariseur, le photon ne passe pas et on enregistre un 0. Pour toute orientation, il existe une certaine probabilité comprise entre 0 et 1 que le photon passe à travers.

La polarisation absolue des photons a une direction totalement aléatoire, par rapport à celle du polariseur, de sorte que dans la configuration originale ($\vartheta = 0$), chaque détecteur enregistre une série de 0 et de 1. Supposons que les séries se présentent de la façon suivante ;

A : 01101011000010110111001100010111 0···

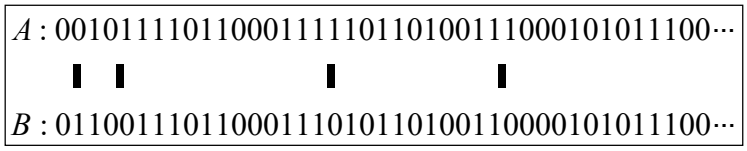
B : 01101011000010110111001100010111 0···

C'est exactement la même chose que dans le cas du canon à clous. Les séries sont identiques, parce que les deux photons d'une même paire possèdent une polarisation identique et que l'angle entre les polariseurs est égal à 0. De plus, chaque série comporte un nombre égal de 0 et de 1, puisqu'un photon a autant de chance d'atteindre le détecteur que de ne pas y parvenir.

[Si $\vartheta = 0,$ il est certain que les deux séries seront identiques ; par contre, il n'y a aucune raison qu'elles comportent le même nombre de 0 et de 1 : 1 signifie que le photon est passé par la fente, et ceci est proportionnel à la taille de la fente, qui n'apparaît pas ici. En tout état de cause, le nombre de 1 devrait être très faible devant le nombre de 0, sauf si la fente est très large ; déjà ici, on constate une description insuffisante de l'appareil de mesure.]

A présent, faisons pivoter le polariseur A d'un angle $\vartheta = 25°.$ Du coup, les deux photons d'une même paire n'ont plus tous les deux exactement la même probabilité d'atteindre les polariseurs et d'être détectés [*A priori, si : les lancements se faisant dans des directions aléatoires selon une loi uniforme, la probabilité du premier d'atteindre sa fente est la même que pour le second, et ce quel que soit l'angle des fentes*].

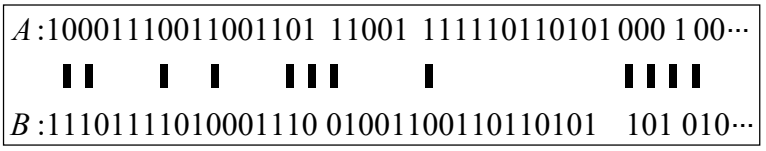
Les séries ne sont donc plus entièrement identiques, elles présentent de temps en temps des « erreurs » de corrélation [*des différences*]. Cependant, en moyenne, les séries A ou B comportent le même nombre de 0 et de 1, parce que la probabilité de passage dans le polariseur est indépendante de son orientation [*la probabilité de passer par une fente est indépendante de l'orientation, puisque les lancers ont des directions selon une loi uniforme : c'est précisément ce que nous venons de dire plus haut].* On a maintenant le résultat :



Nous avons signalé d'une flèche les « erreurs » de corrélation [*ce ne sont pas des erreurs, mais des différences*]. Dans l'exemple ci-dessus, il y a 4 erreurs sur 40 événements, de sorte que le taux d'erreur est $E(\vartheta)=10\%$.

Pour l'instant, l'expérience des photons ressemble à celle du canon à clous. Les photons se comportent comme des clous, comme des objets visualisables. Si nous supposons que l'état de polarisation des photons en A et B est objectif –hypothèse d'objectivité– et qu'une mesure en A n'affecte pas les événements en B -hypothèse de causalité locale, cette expérience doit satisfaire à l'inégalité de Bell $E(2\vartheta)\leq 2E(\vartheta)$.

Or, si nous doublons l'angle pour avoir $2\vartheta=50°$, nous obtenons le résultat suivant :



soit 12 erreurs sur 40 événements et donc $E(2\vartheta)=30\%$. Mais nous avions $E(\vartheta)=10\%$, $2E(\vartheta)=20\%$ l'inégalité de Bell $E(2\vartheta)\leq 2E(\vartheta)$ n'est donc pas vérifiée.

L'inégalité de Bell est donc contredite par cette expérience portant sur des photons. Conclusion :
- ou l'hypothèse d'objectivité est fausse pour les photons ;
- ou bien c'est celle de causalité locale ;
- ou encore les deux à la fois

Voilà qui est très remarquable !

B. Commentaire de la SCM

C'est surtout l'absurdité du raisonnement qui est remarquable. L'auteur ne semble pas remarquer que son expérience "clous" et son expérience "photons" donnent des résultats radicalement divergents et irréconciliables. Expliquons ceci :

Dans l'expérience clous, nous avons une fente d'une certaine largeur (largeur angulaire, notée 2ε dans la première partie). Nous constatons que la probabilité de différence est constante dès que l'angle entre les deux instruments de mesure dépasse une certaine valeur :

$$p_d(\vartheta)=\frac{4\varepsilon}{\pi} \text{ si } \vartheta\geq 2\varepsilon.$$

Cette constatation est très intuitive : si la fente fait 2°, la tourner de 20° ou 30° ne change rien : aucun segment (ou clou) ne peut passer par les deux à la fois ; il y a différence si l'un des segments passe par la fente, ce qui implique automatiquement que l'autre ne le peut pas, puisque les segments sont alignés et que les fentes ne le sont pas.

En mécanique quantique, en admettant la représentation par fonction d'onde et le formalisme hilbertien, on démontre que la probabilité de probabilité de mesurer simultanément le photon 1 avec la polarisation V_α et le photon 2 avec la polarisation V_β est donnée par la formule :

$$P\left(V_\alpha, V_\beta\right) = \frac{1}{2}\cos^2\left(\alpha - \beta\right)$$

Ici, l'un des polariseurs est vertical et l'autre fait un angle α ; la formule se réduit donc à :

$$P\left(V_\alpha, V_0\right) = \frac{1}{2}\cos^2\left(\alpha\right)$$

Il est complètement évident que cette quantité n'est jamais constante, à la différence de la précédente : la comparaison avec un émetteur de clous n'est donc pas pertinente. Cela n'a rien à voir avec des hypothèses d'objectivité ou de causalité, ni avec des variables cachées !

Essayons de comprendre en quoi consiste le dispositif "photons" et en quoi il diffère du dispositifs "clous".

5. Emetteur

Dans le cas des clous, on comprend bien le principe : les clous sont émis avec une orientation aléatoire selon une loi uniforme, deux clous d'une même paire ayant la même orientation. Les clous se propagent sans changer d'orientation.

Dans le cas des photons, on ne comprend pas le principe de l'émission : comment est-on certain que l'émission se fait selon une loi uniforme, comment est-on certain que les deux photons ont exactement la même orientation, et comment sait-on que cette orientation ne se modifie pas au cours du trajet ?

6. Récepteur

Dans le cas des clous, on comprend bien quelle est la géométrie de la fente : il y a une certaine tolérance, caractérisée par l'angle ε ci-dessus.

Dans le cas des photons, on ne comprend pas quelle est la tolérance. D'où sort le calcul de la probabilité, pour un angle α donné ? La configuration du récepteur (taille de la fente) doit bien intervenir, d'une façon ou d'une autre ; ce n'est pas mentionné.

L'article utilise une argumentation qui est en contradiction fondamentale avec les concepts de la mécanique quantique. Citons à nouveau :

"Un positronium est un "atome" constitué d'un seul électron lié à un positron (ou anti-électron) ; cet "atome" se décompose, de façon totalement aléatoire, en deux photons émis dans des directions opposées, et (c'est là le point crucial), dont les polarisations relatives sont ***exactement corrélées*** *- tout comme celles des clous."*

En mécanique quantique, tout est probabiliste ; il est donc impossible que les polarisations des deux photons soient exactement identiques. Au moment de l'émission, la polarisation du second diffère de celle du premier selon une certaine loi de probabilité ; on peut admettre que le maximum est en 0, et que la probabilité décroît avec l'angle.

Ensuite, il faudrait vérifier que la polarisation reste constante dans le temps ; pourquoi ne varierait-elle pas entre l'émission et la réception ?

Nous reprenons la lecture de l'article et abordons la conclusion.

III. Conclusion

A. Retour à l'article

Originellement, John Bell cherchait un moyen de tester l'hypothèse de variables cachées dans le monde quotidien, celui des tables, des chaises, des cailloux. Cela le conduisit à montrer que le fait que son inégalité soit violée par la théorie quantique n'excluait pas forcément l'idée d'un monde objectif décrit par des variables cachées, à condition toutefois que la réalité décrite par ces variables soit non-locale. Rien ne s'oppose à ce qu'existe, par- delà la réalité quantique, une autre réalité, décrite par des variables cachées, dans laquelle les influences s'exerceraient instantanément et sur n'importe quelle distance, sans médiation évidente. Certes, il est possible de croire que le monde quantique est objectif – ce que souhaitait Einstein – mais alors il faut accepter les influences non-locales – à quoi Einstein et la plupart des physiciens se refusent.

Pour comprendre de manière intuitive comment l'objectivité implique la non-localité, comparons les résultats obtenus avec $\vartheta = 25°$ et $\vartheta = 50°$. Il y a beaucoup plus d'erreurs [*ce ne sont pas des erreurs, mais des différences*] lorsque $\vartheta = 50°$ que lorsque $\vartheta = 25°$: 12 contre 4 [*ceci montre bien que l'analogie avec les clous n'est pas correcte].*

On dirait que le fait d'avoir tourné le polariseur *A* a influencé la polarisation des photons qui doivent être détectés par *B*, produisant ainsi toutes ces erreurs "supplémentaires", responsables du fait que l'inégalité de Bell est contredite. Imaginons que l'observateur *B* se trouve sur Terre et l'observateur *A* sur une galaxie lointaine à des années-lumière de là. Tout se passe comme si en faisant pivoter le polariseur *A*, on avait émis un signal plus rapide que la lumière, capable de modifier instantanément le résultat de *B*.

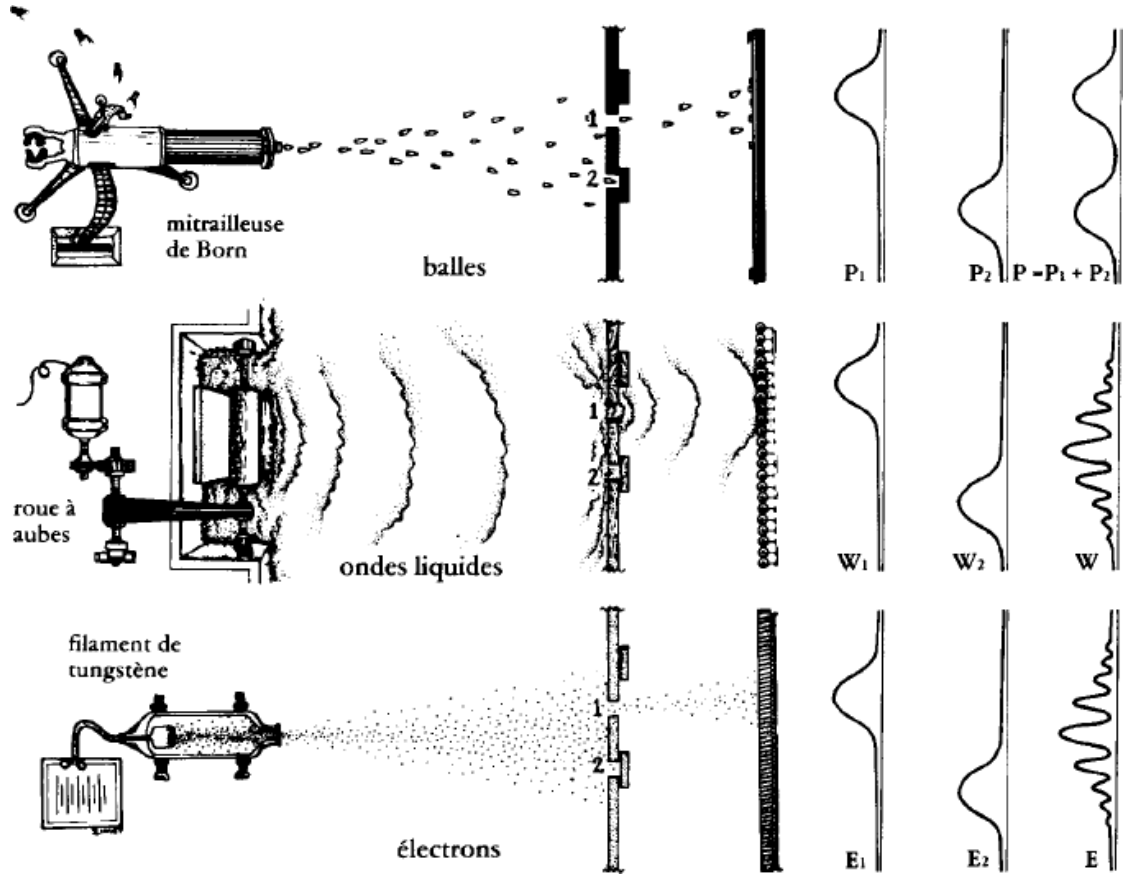
Au point où nous en sommes (la fin de la localité !), il nous faut aller plus avant, car aucun des termes de l'alternative – une réalité non objective ou une réalité non-locale – n'est acceptable. Certains vulgarisateurs des travaux de Bell confrontés à cette alternative n'ontpas hésité à proclamer qu'il s'agissait d'une vérification de la télépathie et que toutes les parties de l'univers étaient instantanément liées les unes aux autres. D'autres en ont conclu qu'il

existait un mode de communication plus rapide que la lumière. Tout cela n'a pas de sens ; la théorie quantique et l'inégalité de Bell n'impliquent rien de tel. Ces commentateurs ont simplement pris leurs désirs pour des réalités.

Pour en arriver à la conclusion que les photons sont soumis à des influences non- locales, nous nous sommes une fois de plus laissés aller à les imaginer dans un état bien défini. Ce n'est que si nous pouvons montrer que les photons existent bel et bien dans un état défini de polarisation, sans pour autant modifier cet état, que nous pourrons dire que l'expérience de Bell manifeste l'existence d'influences non-locales.

La vérification est aisée, lorsqu'il s'agit de clous – il suffit d'installer une caméra à défilement très rapide et de filmer les clous lorsqu'ils arrivent près des polariseurs. Cela ne troublera en rien leur état. Le problème, c'est que l'expérience du canon à clous ne contredisait pas l'inégalité de Bell, ce qui n'est pas le cas avec l'expérience des photons.

Si nous essayons à présent de vérifier l'état de polarisation d'un photon, nous voyons que ce n'est pas possible sans du même coup modifier les conditions initiales de l'expérience, à savoir que deux photons d'une même paire doivent avoir des polarisations identiques. Lorsque nous mesurons la polarisation d'un photon, nous le plaçons dans un état défini, ce qui change les conditions initiales de l'expérience. C'est exactement la même chose que dans l'expérience des deux trous de Young : en observant grâce à une source lumineuse placée derrière le trou par quel trou l'électron est passé, nous avons là aussi modifié la figure observée sur l'écran.



Sous ses trois formes, l'expérience des deux trous d'Young : la mitrailleuse de Max Born, les ondes liquides et les électrons.

Autant il nous est possible de représenter comment les balles et les ondes liquides (objets relevant de la physiqueclassique) produisent les résultats observés sur les écrans de détection, autant il nous est impossible de représenter ce qui advient aux électrons (particules quantiques) au niveau des deux trous.

De même, ici le fait de déterminer l'état objectif du photon modifie les conditions dans lesquelles a été établie l'inégalité de Bell. Toute tentative pour vérifier expérimentalement l'hypothèse d'objectivité entraîne une modification des conditions expérimentales telle que nous ne pouvons plus nous servir de la violation de l'inégalité de Bell pour conclure à l'existence d'influences non-locales.

Supposons donc que nous ne tentions pas de vérifier l'état des photons. Après tout, nous connaissons les résultats de l'expérience en *A* et en *B* et ces renseignements qui font partie du monde macroscopique au même titre que les tables, les chaises et les chats sont certainement objectifs. L'observateur placé en *B* ne peut-il lire le résultat, voir que l'inégalité de Bell est contredite et en conclure que la causalité locale est également contredite ? Eh bien, non car souvenons-nous que la source émet des photons par paires, avec une polarisation aléatoire. Cela signifie que les enregistrements effectués en *A* et en *B* constituent des séquences totalement aléatoires de 0 et de 1, quel que soit l'angle choisi.

A première vue, nous pourrions croire qu'en modifiant le polariseur en *A*, nous avons directement influé sur le nombre d'erreurs enregistrées en *B*. Mais alors, rien qu'en modifiantde diverses façons le polariseur en *A* et en étudiant les modifications du nombre d'erreurs enregistrées en *B*, l'observateur en *B* pourrait décrypter un message envoyé par *A*. On obtiendrait ainsi un télégraphe contraire à la notion de causalité.

Mais en réalité, aucune information de ce type ne peut être transmise de *A* à *B* à l'aide d'un tel système, car avec un seul et unique enregistrement d'événements, soit en *A,* soit en *B,* nous ne sommes guèreplus avancés que si nous possédions un message ultra secret rédigé dans un code aléatoire –un tel message est impossible à déchiffrer. Ainsi donc, du fait que les séquences enregistrées en *A* et en *B* sont totalement aléatoires, il n'est pas possible de communiquer entre *A* et *B*. il n'y a donc pas de non-localité.

Deux séquences aléatoires peuvent fournir une information non aléatoire lorsqu'elles sont comparées l'une à l'autre. L'information se trouve dans la corrélation née de la comparaison. Il en va de même avec les enregistrements effectués en *A* et en *B :* l'information concernant l'angle relatif des polariseurs est inscrite dans la corrélation des deux enregistrements, mais pas dans chaque enregistrement pris individuellement. Lorsqu'on modifie l'angle du polariseur, une séquence aléatoire est transformée en une autre séquence aléatoire et il est impossible de dire ce qui se passe en n'étudiant qu'un seul enregistrement. Ce type de processus aléatoire se déroule effectivement dans la nature, et c'est pour cela que nous rejetons l'idée d'une véritable non-localité.

Modifiée de manière aléatoire, une séquence aléatoire reste une séquence aléatoire ! – le

désordre reste désordonné. C'est précisément ce qui se passe dans le cas des séquences aléatoires enregistrées en *A* et *B*. Par contre, la comparaison des séquences permet de savoir que les conditions expérimentales ont été modifiées du fait des mouvements des polariseurs – l'information réside dans la corrélation, pas dans les enregistrements individuels. Cette corrélation est entièrement prévue par la théorie quantique.

En conclusion, l'expérience de Bell n'implique pas l'existence de véritables influences non-locales, même si nous acceptons l'objectivité du monde microscopique. Elle implique simplement que l'on peut modifier instantanément la corrélation de deux séquences aléatoires d'événements survenus aux deux extrémités de la galaxie. Mais la corrélation de deux ensembles d'événements très éloignés les uns des autres ne constitue pas un objet local et l'information qu'elle peut contenir ne peut servir à contredire le principe de causalité locale.

Avec l'inégalité de Bell et l'expérience d'EPR, nous avons pénétré au cœur même de "l'étrangeté quantique".

B. Commentaire SCM

Il n'est pas nécessaire d'invoquer un principe de "causalité locale" ou d'"étrangeté quantique" : les photons ne sont pas nécessairement polarisés exactement dans la même direction ; les principes fondamentaux de la mécanique quantique s'y opposent clairement. Il faudrait disposer d'une densité de probabilité portant sur l'angle possible entre la polarisation de A et celle de B ; si cette loi n'est pas explicitée, tout le reste est dépourvu de valeur explicative.

Il faudrait aussi expliciter la nature des fentes et leur largeur : quel est l'angle admissible, pour un photon polarisé, pour qu'il accepte de passer par une fente verticale ? Il n'est pas évident, du reste, que cette tolérance soit la même pour toutes les inclinaisons : la Nature n'est pas nécessairement invariante par rotation.

Nous pouvons rejoindre la position d'Albert Einstein : il y aurait une explication assez simple au fait que deux photons intriqués révèlent la même polarisation lorsqu'ils sont mesurés. Prenons pour simplifier le cas de deux valeurs possibles (comme pour le spin de l'électron). Admettons que l'électron ait deux "couleurs" possibles, rouge et bleu (c'est ce que Einstein appelait "variable cachée"). Lors de l'intrication, les deux éléments de la paire sont assujettis à être de la même couleur, qu'ils garderont toute leur vie, et au moment de la mesure, la couleur détermine le spin.