LA THEORIE QUANTIQUE DE L'INFORMATION.

Aperçu des lois qui régissent le monde quantique.

Werner Heisenberg

Paul Dirac

Erwin Schrödinger

Au delà du déterminisme et du réalisme ?

Au niveau atomique, les lois physiques paraissent très différentes de ce qu'elles sont à notre échelle. De fait, les photons et les particules élémentaires, électrons, protons et neutrons, de même que les édifices qu'elles construisent par assemblages immédiats, atomes et molécules, se comportent très différemment des objets qui peuplent le monde macroscopique.

Si nous n'avons pris conscience de ce fait qu'assez tardivement, c'est parce que la physique s'est, historiquement, développée à reculons en partant des modèles valides à l'échelle humaine. A notre échelle, billes, pendules, aimants, …, évoluent dans l'espace-temps en suivant des trajectoires bien définies que des équations d'évolution, qui tiennent compte des interactions avec l'environnement, permettent de prédire à partir d'un nombre suffisant de conditions initiales, typiquement de position et de vitesse. L'ensemble des interactions mécaniques et électromagnétiques forment le corpus de la physique classique.

Les lois de la physique classique sont déterministes. Cela signifie que l'évolution de n'importe quel système classique peut être prédite avec une précision arbitrairement grande pourvu que les conditions initiales soient connues avec une précision « suffisante ». On rappelle que la signification du mot « suffisante » varie selon que le système considéré est chaotique ou non :

- Si le système n'est pas chaotique, la précision de la prédiction sera, en mettent les choses au pis, une fonction polynomialement croissante (heureusement souvent linéaire) de la précision des données. Ainsi en va-t-il d'une planète orbitant autour d'une étoile fixe (c'est le cas le plus favorable car ce mouvement est périodique), d'une boule de billard circulant sans frottement sur la surface plane d'un billard circulaire ou encore d'un pendule simple sans frottement.

- Si le système est chaotique, il faut craindre que cette prédiction soit épisodiquement une fonction exponentiellement croissante de l'imprécision des données. Ce serait le cas de la même boule de billard circulant sur un billard en forme de stade ou du pendule attaché à une corde élastique.

La dynamique des systèmes physiques macroscopiques, chaotiques ou non, est non seulement déterministe mais encore réaliste. On entend par là que, même enfermé dans une boîte noire dont le contenu serait inaccessible, personne ne doute de la réalité objective d'un mécanisme qui en commande l'évolution. Pour tout scientifique réaliste, découvrir les rouages de ces mécanismes n'est qu'une question de temps et de moyens expérimentaux.

L'image est suggestive d'une médecine qui découvre, au cours des siècles, l'élévation anormale de la température du corps et invente le terme « infection », ce qui est une façon savante d'avouer qu'on ne comprend pas ce qui se passe. Le médecin réaliste croît cependant en l'existence d'un agent responsable qu'il baptise microbe et une fois qu'il l'a trouvé, soigne par extermination. Toutefois, la médecine n'a pas toujours été réaliste. A condition de remonter suffisamment loin dans le temps (en fait pas si loin que cela !), la maladie était perçue, au choix, comme une punition du ciel, un miasme ambiant, …, le détail de l'énumération est sans intérêt. Entre superstition et réalisme, un troisième courant, dit positiviste, a vu le jour qui, dans le cas de la médecine, s'en est tenu aux faits observables sans penser à l'éventualité d'une cause sous-jacente. C'est cette médecine positiviste qui a soigné nos arrières grands-parents par traitement du symptôme et non de l'agent responsable.

Le positivisme a-t-il une raison d'être en physique ? La question peut choquer si l'on croît dur comme fer, comme le faisait Einstein, qu'il existe toujours un élément de réalité objective, éventuellement provisoirement hors d'atteinte, qui régit l'évolution des systèmes.

Si le système étudié est macroscopique tout le monde est d'accord qu'il est déterministe et chacun admet, sans effort, que même enfermé dans une boîte noire, il se trouve toujours dans cette boîte les éléments de réalité qui en expliquent l'évolution. Même si le système est chaotique et qu'il se comporte pseudo-aléatoirement une partie de son temps, personne ne doute que ce comportement erratique résulte, en fait, de l'évolution instable de quelques variables cachées qui décrivent le système.

Si le système est nanoscopique, le débat change radicalement. A l'échelle atomique, les objets se comportent systématiquement aléatoirement. Par exemple, un noyau radio-actif α émet ces particules à des intervalles de temps irréguliers et imprédictibles sauf qu'ils respectent une loi générale de décroissance moyenne exponentielle. Les physiciens réalistes aimeraient penser que ce hasard est de la même veine que celui des systèmes chaotiques et qu'il se trouve à l'intérieur des noyaux quelques mécanismes non découverts obéissant à une dynamique suffisamment instable.

Mais les derniers décennies du XXème siècle semblent avoir montré que cette piste n'est sans doute pas la bonne et qu'à ce stade, le courant positiviste défendu par Bohr prend une revanche éclatante : dans le monde quantique, le hasard paraît fondamental et résiste à toute tentative d'explication en terme de variables cachées. En d'autres termes, on peut l'observer, procéder à des mesures et prédire les probabilités d'issue de toute nouvelle expérience mais la question est et restera vide de sens de se demander quels mécanismes se cachent derrière cet indéterminisme radical. La théorie quantique est le modèle qui décrit correctement l'évolution des systèmes à l'échelle atomique.

La complexité du monde quantique.

Tout système quantique est caractérisé par quelques propriétés qui le rendent réfractaire à la compréhension intuitive classique : le probabilisme, l'interférence, l'intrication et l'indiscernabilité.

- Dans l'expérience d'Young, lorsqu'un photon unique (ou une particule élémentaire quelconque) traverse un système de deux fentes étroites et rapprochées, il est impossible de prédire en toute certitude lequel des nombreux détecteurs placés en aval enregistrera l'arrivée de la particule. Seule la probabilité de détection attachée à chaque détecteur peut être calculée a priori et les règles de la mécanique quantique permettent de faire cette prédiction. Ce probabilisme est essentiel et irréductible à toute cause cachée. Dans l'état actuel de nos connaissances, « Dieu semble jouer aux dés ».
- Par ailleurs, dans l'expérience précédente et selon la théorie quantique, le seul événement à prendre en considération est la détection de la particule par celui des détecteurs qui en a conservé une trace sensible et objective. Par contre, la question est vide de sens de se demander par quelle ouverture la particule est réellement passée : c'est, en effet, un non-événement car il n'a laissé aucune trace sensible au niveau d'une des fentes. A ce titre, il

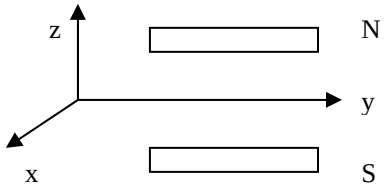
n’a pas à être pris en considération dans les calculs de prédiction quantique. Ces calculs s’effectuent, au contraire, en assumant que la particule emprunte potentiellement les deux trajets comme s’ils ne formaient qu’une seule trajectoire intriquée puis en calculant, selon des règles appropriées, le résultat de l’interférence entre ces deux possibilités. Si on tente une mesure auxiliaire destinée à voir par quelle fente la particule est réellement passée, on perturbe le système à tel point que l’interférence disparaît en sorte qu’on ne parle plus du tout de la même expérience.

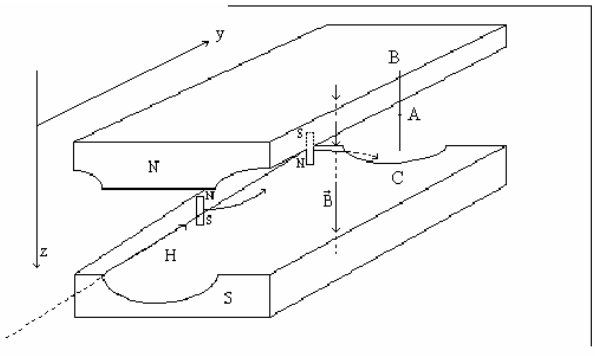
- Enfin, deux objets quantiques identiques et confinés dans une région de l’espace perdent toute notion d’individualité. La raison en est que la notion de trajectoire n’existe plus en mécanique quantique. C’est une conséquence du principe d’incertitude sur lequel nous aurons à revenir. Il en résulte que lorsque deux particules identiques, A et B, se rapprochent puis s’éloignent, il est vide de sens de se poser la question de savoir qui est A et qui est B à la sortie. La vérité est que des particules identiques sont indiscernables et qu’elles forment ensemble un système inséparable. Par exemple, deux photons de même fréquence émis simultanément par un seul atome sont indiscernables dès la naissance et ils doivent être traités par le modèle théorique comme s’ils ne formaient qu’un seul objet intriqué, quelle que soit la distance qui les sépare. Cela reste vrai tant que le reste de l’univers ne perturbera pas leur cohérence interne. De même, deux électrons prisonniers d’un atome d’hélium forment un système indissociablement intriqué. Seul le milieu extérieur peut à nouveau espérer rompre cette cohérence dans l’intrication.

Ce n’est que lorsqu’on assemble un nombre suffisant d’objets quantiques qu’on fabrique des objets de dimensions croissantes qui perdent progressivement leur cohérence au contact du milieu extérieur. Leurs comportements rejoignent alors ceux que prédisent les lois de la physique classique.

L’expérience de Stern-Gerlach.

Une expérience célèbre condense, à elle seule, quelques uns des ingrédients nécessaires au développement de l’intuition quantique. On la décrit schématiquement comme suit. De l’argent métallique est chauffé dans un four jusqu’à obtenir des atomes de vapeur qu’on éjecte par une petite ouverture le long d’un axe Oy soigneusement collimaté. On fait passer ces atomes dans l’entrefer d’un électro-aimant puissant dont le profil garantit un gradient intense d’induction selon l’axe transversal, Oz.





Un atome d'argent est électriquement neutre et, dans son état fondamental, il ne possède aucun moment magnétique orbital. On s'attendrait donc à ce qu'il reste insensible au champ magnétique et poursuive son chemin sans être dévié pour aboutir au point A sur l'écran d'observation. La réalité expérimentale est différente : les atomes sont individuellement et aléatoirement déviés dans la direction des z positifs ou négatifs et ce dans une proportion 50-50 : ils dessinent deux zones d'impacts bien contrastées, en B et en C sur la figure. La suite que l'on observe, {BBCBCCCBCBBB…}, est complètement aléatoire au sens que la théorie de l'information prête à ce terme : sa complexité algorithmique vaut exactement 1bit/symb.

On interprète ces observations en posant que l'atome d'argent possède un moment magnétique interne, μ_z. C'est l'électron de valence de l'atome qui est porteur de ce moment, dit de spin, et l'atome en hérite tout naturellement. A ce stade on pourrait penser avoir compliqué inutilement les choses en utilisant des atomes d'argent. Pourquoi ne pas recommencer l'expérience directement avec des électrons ? Cela serait certainement possible mais le fait que l'électron soit chargé introduit une complication supplémentaire : il serait en plus très fortement dévié par le champ magnétique, dans le plan Oxy, et sauf à profiler l'entrefer en arc de cercle, il échapperait immédiatement au gradient d'induction.

Le fait que certains atomes soient déviés vers le haut et d'autres vers le bas, résulte sans doute d'une orientation différente des moments magnétiques individuels par rapport à l'axe Oz. On le comprend en remplaçant les atomes par de petits aimants classiques, orientés au hasard : le gradient d'induction entraîne toujours une résultante de force, $F_z = \mu_z(\partial B_z / \partial z)$, orientée, selon Oz, dans un sens ou dans l'autre selon le signe de μ_z. Toutefois la comparaison avec des aimants classiques s'arrête là car des aimants orientés au hasard devraient faire apparaître une traînée continue d'impacts le long du segment BC et pas des impacts isolés à ses extrémités.

De plus, la direction de l'axe Oz de l'analyseur ne joue aucun rôle particulier dans cette expérience, sauf qu'elle est perpendiculaire à l'axe Oy de propagation. Or si l'on fait tourner l'analyseur d'un angle, θ, quelconque autour de l'axe Oy, on constate que les impacts de détection sur l'écran tournent eux aussi du même angle en sorte que μ_z exhibe en permanence une des valeurs, $\pm\frac{1}{2}\ (\mu_B)$!

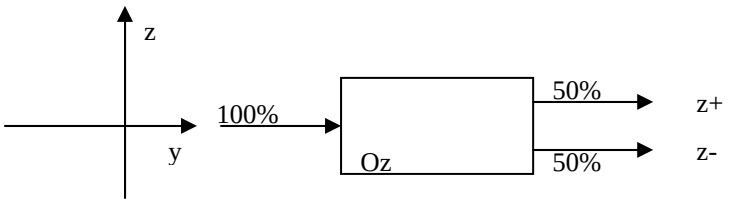
De toute évidence l'analyseur joue un rôle inattendu. La théorie quantique interprète ces résultats en posant que l'analyseur (= l'électro-aimant) trie aléatoirement les atomes en deux catégories seulement, caractérisées par des moments magnétiques, μ_z, dont la valeur peut être déduite de l'écartement des points B et C (μ_B est le magnéton de Bohr) :

$$\mu_z = \pm\frac{1}{2}\ (\mu_B).$$

On voit que cette interprétation pose immédiatement un problème à l'intuition : le caractère aléatoire des observations n'est pas uniquement imputable à la source : l'analyseur y ajoute sa contribution.

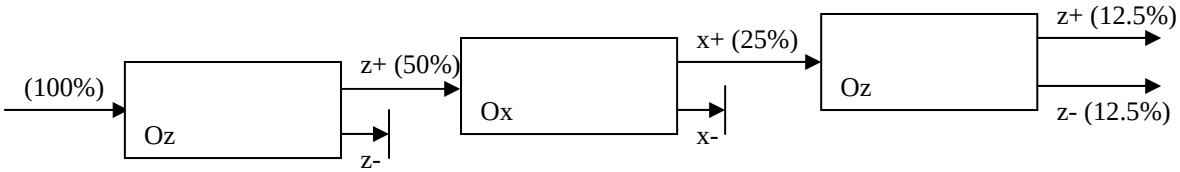
On peut tenter d'y voir plus clair en poursuivant l'investigation expérimentale. On découvre alors qu'il faut effectivement faire table rase de l'intuition développée au contact du monde macroscopique. Voici les faits.

On découvre une autre source d'étonnements lorsqu'on enchaîne en série plusieurs analyseurs. Une difficulté expérimentale se présente toutefois à ce stade du fait qu'il ne suffit malheureusement pas de disposer les analyseurs les uns derrière les autres. En effet les atomes qui traversent le premier électro-aimant sont inévitablement déviés vers le haut ou vers le bas. Imaginons que nous continuions à travailler sur le faisceau supérieur. Ce faisceau suit maintenant une trajectoire selon un axe Oy' qui ne coïncide plus avec l'axe Oy et du coup l'axe Oz s'en trouve modifié lui aussi. Nous n'entrerons pas dans les détails techniques nécessaires à la rectification de la trajectoire du faisceau dans l'alignement Oy primitif. On trouvera dans le cours de Feynman une solution envisageable mais il nous suffit de savoir que cela est possible. Nous représenterons schématiquement comme suit l'analyseur rectifié :



Considérons un premier analyseur de Stern-Gerlach qui sépare le faisceau initial en deux sous-faisceaux filtrés chacun dans une valeur du moment magnétique, $+\frac{1}{2}\ (\mu_B)$ ou $-\frac{1}{2}\ (\mu_B)$, mesuré selon l'axe Oz. Pour abréger les notations, nous notons provisoirement, z+ et z-, les états filtrés correspondants. Eteignons le faisceau z-, par exemple à l'aide d'un écran absorbeur et faisons passer le faisceau restant, z+, dans un deuxième analyseur orienté comme le premier. On constate que tous les atomes sont déviés vers le haut ce qui indique qu'ils demeurent filtrés dans l'état z+, comme on pouvait l'espérer. Par contre, si le deuxième analyseur est tourné de 90° autour de Oy, dans un sens ou dans l'autre, en sorte que son axe bascule dans la position Oz' = ±Ox, on constate que les atomes sont aléatoirement et équitablement déviés dans les directions positive et négative de Ox.

Il y a encore plus fort, si on absorbe le sous-faisceau orienté selon x- et qu'on fait repasser celui qui reste dans un troisième analyseur orienté comme le premier, on observe à nouveau des déviations aléatoires selon z+ et z-. Tout se passe comme si les atomes ne se souvenaient plus du premier filtrage qu'ils ont subi !



Cette série d'expériences semble indiquer que l'analyseur choisit aléatoirement les valeurs observées parmi quelques valeurs autorisées, deux dans le cas du spin de l'électron, autrement dit, que l'analyseur fonctionne comme un filtre de mesure aléatoire. On sait que, d'une manière générale, toute mesure perturbe le système auquel elle s'adresse. C'est sans

conséquence en physique classique car les systèmes sont de grande taille et on peut toujours s'arranger pour que la perturbation soit rendue aussi petite que l'on veut et en tous cas inférieure à la précision des étalons utilisés. Mais cela cesse d'être vrai lorsqu'on mesure une propriété d'un système qui se situe tout en bas de l'échelle dimensionnelle. Dans ce cas, la perturbation peut atteindre le même ordre de grandeur que celui de la variable que l'on mesure à tel point que le résultat de cette mesure paraît aléatoire. Le moment est venu d'exposer les principes de la théorie qui décrit correctement les comportements observés à l'échelle nanoscopique.

Les principes de la mécanique quantique.

Il existe un modèle théorique qui décrit correctement l'expérience de Stern-Gerlach et qui prédit tout aussi correctement les phénomènes quantiques connus. Nous le présentons de façon informelle en adoptant la notation de Dirac. Chaque principe, aussitôt énoncé, sera illustré par l'exemple d'une particule chargée présentant deux états de moments magnétiques, en l'occurrence l'électron.

1) Principe d'observabilité. La physique quantique ne veut et ne peut répondre qu'à des questions dont l'issue est expérimentalement observable et mesurable. Toute autre sorte de question est considérée comme ésotérique, mal posée et, de ce fait, vide de sens. Dans le même ordre d'idée, un événement qui n'a fait l'objet d'aucune mesure effective doit être considéré comme un non-événement qui ne possède pas de réalité objective.

Exemple : il est dénué de sens de se demander quelle forme ou quelles dimensions caractérisent un électron. Préciser la forme de l'électron exigerait en effet de le sonder à l'aide d'un système auxiliaire nettement plus petit que lui, ce qui est inconcevable dès l'instant où l'électron est élémentaire. Par contre, on peut mesurer quelques propriétés discrètes qui le caractérisent, sa charge électrique ou encore son moment magnétique propre. On peut ainsi en déduire indirectement son moment angulaire propre (spin), en l'occurrence $+1/2(\hbar)$ ou $-1/2(\hbar)$. De fait, le spin d'une particule élémentaire ne peut être mis en évidence par voie directe, donc mesuré, que si cette particule est chargée : un moment magnétique est alors associé au spin qui lui est directement proportionnel. Dans le cas des particules non chargées il faut travailler autrement, par exemple en invoquant les lois de conservation.

Par ailleurs, lorsqu'une source émet un électron, il n'y a pas lieu de penser qu'il possède, relativement à Oz, soit le spin +1/2 soit le spin –1/2. Sauf le cas, qui ne nous intéresse pas actuellement, où il aurait reçu une préparation préalable dans un de ces états particulier, il y a plutôt lieu de le considérer comme potentiellement présent dans les deux états simultanément. Cette logique quantique où une porte n'est pas nécessairement ouverte ou fermée peut surprendre et on pourrait croire qu'on la mettrait en difficulté en effectuant une mesure qui, de fait, exhiberait une valeur et une seulement, +1/2 ou –1/2. Toutefois ce serait une erreur de penser que cette réponse révélerait une valeur préexistante. Le rôle de la mesure quantique est très différent de celui d'une mesure classique : la perturbation qu'elle exerce sur le système est tellement violente qu'elle agit comme un véritable tirage au sort parmi toutes les valeurs autorisées par le principe de l'observable exposé sous peu. Quant à la valeur « réelle » du spin à la sortie de la source, personne ne la connaîtra jamais et le fait est que la question est sans objet.

2) Principe de la description d'état. La mécanique quantique développe la description des systèmes dans le cadre des espaces vectoriels de Hilbert. Ce sont des espaces vectoriels semblables à bien des égards à l'espace ordinaire, à trois dimensions, sauf quelques changements qui n'altèrent heureusement pas trop l'ensemble des notations auxquelles on est habitué :

- le nombre des dimensions peut être quelconque allant de deux à l'infini,
- les composantes des vecteurs de même que les scalaires peuvent être complexes.

L'état d'un système élémentaire, une particule par exemple, est indifféremment décrit par un vecteur dit « ket », $|v\rangle$, à n dimensions (n pouvant être infini) ou par son dual, dit « bra » $\langle v|$. Dans une représentation matricielle, toujours agréable, les vecteurs « kets » peuvent être assimilés à des vecteurs colonnes tandis que les « bras » correspondants sont leurs adjoints, donc les vecteurs lignes obtenus en transposant et en conjuguant les « kets » correspondants. Chacun condense, à sa façon, l'information nécessaire à la description complète de la particule y compris son état de mouvement. Tout vecteur d'état est développable selon les vecteurs, $|b_i\rangle$, d'une base orthonormée quelconque qui fait apparaître leurs composantes selon cette base :

$$|v\rangle = \sum_i c_i |b_i\rangle \qquad \Leftrightarrow \qquad \langle v| = \sum_i c_i^* \langle b_i| .$$

Un produit scalaire est défini entre « bras », $|v\rangle = \sum_i c_i |b_i\rangle$, et « kets », $\langle u| = \sum_j d_j^* \langle b_j|$, noté :

$$\langle u|v\rangle = \langle v|u\rangle^* = \sum_i \sum_j d_j^* c_i \langle b_j|b_i\rangle = \sum_i \sum_j d_j^* c_i \delta_{i,j} = \sum_i d_i^* c_i .$$

La définition de la norme, réelle et positive, de $|v\rangle$ en découle : $\langle v|v\rangle = \langle v|v\rangle^* = \sum_i |c_i|^2$.

Dans la décomposition selon une base, $|v\rangle = \sum_i c_i |b_i\rangle$, on a que les coefficients, c_i, se calculent comme suit :

$$c_i = \langle b_i|v\rangle .$$

On peut donc réécrire $|v\rangle$ sous la forme : $|v\rangle = \sum_i |b_i\rangle\langle b_i \| v\rangle$..

L'opérateur, $P_i = |b_i\rangle\langle b_i|$, dit « produit extérieur », peut être vu comme l'opérateur qui projette tout vecteur sur le vecteur de base $|b_i\rangle$. Si l'espace de Hilbert est complet, on doit avoir :

$$\sum_i |b_i\rangle\langle b_i| = \hat{1}.$$

Exemple : poursuivons l'exemple de l'électron pour lequel nous avons vu qu'il n'existe que deux états possibles du moment magnétique selon Oz, notés indifféremment, $|z+\rangle = |0\rangle$ et $|z-\rangle = |1\rangle$, et correspondant aux spins, +1/2 et –1/2, dans cet ordre conventionnel. Dans une représentation matricielle de l'espace de Hilbert à deux dimensions, il est commode d'associer ces états aux vecteurs de base :

$$|b_1\rangle = |z+\rangle = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad \text{et} \qquad |b_2\rangle = |z-\rangle = |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$

Les projecteurs, P_i, associés aux vecteurs de base s'écrivent :

$$\hat{P}_1 = |b_1\rangle\langle b_1| = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} \qquad \text{et} \qquad \hat{P}_2 = |b_2\rangle\langle b_2| = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix},$$

et on a bien que la représentation est complète : $\hat{P}_1 + \hat{P}_2 = \hat{1}$.

3) Principe de superposition. Un système nanoscopique, qui n'a fait l'objet d'aucune préparation particulière, doit être considéré comme coexistant potentiellement dans tous les états accessibles à une mesure quelconque et son vecteur d'état s'exprime comme combinaison linéaire des vecteurs de base de l'espace de Hilbert correspondant,

$$|v\rangle = \sum_i c_i |b_i\rangle.$$

Dans cette relation, les coefficients, $c_i = \langle b_1 | v\rangle$, sont réels ou complexes et le carré de leur module vaut la probabilité que le système se retrouve précisément dans l'état, i, au terme d'une mesure effectuée à cet instant :

$$p_i = |\langle b_i | v\rangle|^2.$$

La somme des probabilités devant valoir 1, on voit que $|v\rangle$ doit être normé à l'unité :

$$\langle v|v\rangle = \sum_i |c_i|^2 = 1.$$

Seules les probabilités, p_i, étant calculables, il en résulte que tout vecteur d'état, $|v\rangle$, n'est jamais défini qu'à un facteur multiplicatif inessentiel, $e^{i\varphi}$, près. Autrement dit l'opération, $|v\rangle \rightarrow e^{i\varphi}|v\rangle$ est une opération de symétrie (dite de jauge) du système.

Exemple : lorsqu'un électron est émis par une source n'ayant fait l'objet d'aucune préparation, personne ne peut savoir dans quel état de moment magnétique il se trouve. Il se trouve, en fait, dans un état de superposition quantique noté :

$$|v\rangle = c_1|z+\rangle + c_2|z-\rangle = \begin{pmatrix}c_1\\c_2\end{pmatrix}.$$

Par l'absence de préparation de la source, on signifie qu'aucun expérimentateur malicieux n'a volontairement préparé (donc mesuré !) chaque électron issu de la source dans un état déterminé, par exemple en incorporant subrepticement un analyseur de Stern-Gerlach à la source. Il en résulte que les valeurs exactes des coefficients c_1 et c_2 sont inaccessibles et que la question de connaître leurs valeurs précises n'a, en fait, pas de sens puisque toute tentative de les révéler

impliquerait une mesure destructrice. Précisément, $|c_1|^2$ et $|c_1|^2$ (avec $|c_1|^2 + |c_2|^2 = 1$), représentent les probabilités qu'un analyseur de Stern-Gerlach projette l'électron dans l'un ou l'autre des états, $|z+\rangle$ ou $|z-\rangle$ respectivement, fixant par la même les coefficients c_1 et c_2.

4) Principe de l'observable. Toute grandeur observable et donc mesurable est caractérisée par un opérateur, $\hat{O}$, hermitien qui agit sur les vecteurs d'états, transformant les « kets » en « kets » ou les « bras » en « bras » en suivant les règles suivantes :

$$O|v\rangle = |u\rangle \qquad \Leftrightarrow \qquad \langle v|\tilde{O}^* = \langle u|.$$

Seules les valeurs propres, λ, de cet opérateur, nécessairement réelles, sont observables. Elles sont solutions de l'équation aux valeurs propres :

$$\hat{O}|x\rangle = \lambda|x\rangle.$$

Lorsqu'on cherche à mesurer la grandeur associée à un opérateur, $\hat{O}$, on peut donc être certain que les valeurs observables sont à chercher parmi les seules valeurs propres de cet opérateur. Par contre il est totalement impossible de deviner à l'avance quelle valeur sortira précisément de la mesure : cela est complètement aléatoire. Seule la probabilité qu'une valeur propre particulière soit détectée est calculable selon le protocole suivant : si l'état initial est décrit par le vecteur, $|x\rangle_{avant} = \sum_i c_i |v_i\rangle$, où les v_i forment la base des vecteurs propres relativement à la grandeur mesurée, la probabilité qu'on mesure la valeur propre, λ_i, vaut $|c_i^2|$.

Tout opérateur est décomposable sous forme spectrale en terme des valeurs propres et des projecteurs associés,

$$\hat{O} = \sum_i \lambda_i |v_i\rangle\langle v_i| = \sum_i \lambda_i \hat{P}_i ,$$

d'où il résulte que tout opérateur possède une représentation matricielle.

Exemple : les opérateurs associés aux trois composantes du spin de l'électron s'écrivent :

$$S_x = \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad S_y = \frac{\hbar}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad S_z = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

L'opérateur associé à la composante du moment magnétique, orientée selon Oz, se note :

$$\mathbf{M_z} = \frac{1}{2}\mu_B \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

C'est l'opérateur qui est associé à un analyseur de Stern-Gerlach orienté selon Oz. Si on fait tourner cet analyseur d'un angle, θ, dans le sens direct autour de Oy, il y a lieu de recalculer

l'opérateur correspondant, M_θ, en appliquant l'opérateur de rotation convenable (cfr. annexe 1), soit dans le cas envisagé :

$$M_\theta = R_{y,\theta}^{-1}\mu_B\begin{pmatrix}1/2 & 0\\ 0 & -1/2\end{pmatrix}R_{y,\theta} = \frac{1}{2}\mu_B\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}.$$

5) Principe de la mesure par projection d'état. Toute mesure d'une grandeur physique effectue un tirage au sort parmi les valeurs propres de l'opérateur associé. De plus, lorsqu'une valeur propre est sélectionnée, l'état du système est instantanément projeté sur l'espace des vecteurs propres associés à λ. Techniquement cela signifie que la mesure active l'opérateur de projection associé,

$$\hat{P} = \sum_{\substack{\text{états}\\ \text{propres}(\lambda)}} |v_\lambda\rangle\langle v_\lambda|,$$

et qu'elle transforme le vecteur d'entrée normalisé en un vecteur de sortie renormalisé :

$$|x\rangle_{\text{après}} \underset{\text{renorm}}{=} \hat{P}|x\rangle_{\text{avant}}.$$

Lorsque les valeurs propres sont non dégénérées, ce que nous supposerons afin de ne pas alourdir la présentation, le sous-espace propre se réduit au seul vecteur propre, $|v\rangle$, associé à la valeur propre mesurée et l'opérateur de projection se réduit simplement au produit extérieur :

$$\hat{P} = |v\rangle\langle v| \qquad \Rightarrow \qquad |x\rangle_{\text{après}} \underset{\text{renorm}}{=} |v\rangle\langle v|x\rangle_{\text{avant}}.$$

Du fait que P n'est pas unitaire, cette égalité sous-entend de renormaliser le vecteur d'état, en fait :

$$\hat{P} = |v\rangle\langle v| \qquad \Rightarrow \qquad |x\rangle_{\text{après}} = \frac{|v\rangle\langle v|x\rangle_{\text{avant}}}{\big\||v\rangle\langle v|x\rangle_{\text{avant}}\big\|}.$$

Alors que les opérateurs d'évolution sont unitaires, déterministes et réversibles, les opérateurs de projection activés par les mesures sont non unitaires, probabilistes et irréversibles. Toute mesure effectuée sur un système entérine provisoirement la valeur de la grandeur mesurée et précise le nouveau vecteur d'état en projetant l'ancien sur le sous-espace des vecteurs propres de l'opérateur associés à la valeur propre mesurée. En particulier, si une mesure préalable a préparé le système dans un état propre déterminé, la probabilité qu'il soit détecté dans le même état lors d'une deuxième mesure vaut 1 (certitude) et dans un état différent vaut 0 (impossibilité). L'entérinement provisoire signifie que toute mesure ultérieure de la même grandeur ne peut plus rien changer au fait que le système est désormais décrit par ce vecteur d'état particulier. Nous verrons que cela cesse d'être vrai si on tente ultérieurement la mesure d'une autre grandeur du système qui ne commuterait pas avec la précédente : le vecteur d'état serait modifié dans ce cas.

Exemples : 1) supposons que l'on cherche à mesurer la composante, selon Oz, du moment magnétique d'un électron au moyen d'un analyseur de Stern-Gerlach. Admettons que cet électron est absolument quelconque, en d'autres termes, qu'il n'a subi aucune mesure préalable. Son vecteur d'état initial s'écrit :

$$|\text{in}\rangle = c_1|z+\rangle + c_2|z-\rangle .$$

On sait que le résultat de cette mesure ne peut fournir que les réponses $+1/2(\mu_B)$ et $-1/2(\mu_B)$ mais la valeur exacte est imprévisible. Seule les probabilités d'occurrences respectives de ces deux valeurs sont calculables selon les formules générales :

$$p(+1/2) = \left|\langle \text{in}|z+\rangle\right|^2 = \left|(c_1^* \quad c_2^*)\begin{pmatrix}1\\0\end{pmatrix}\right|^2 = |c_1|^2$$

$$p(-1/2) = \left|\langle \text{in}|z-\rangle\right|^2 = \left|(c_1^* \quad c_2^*)\begin{pmatrix}0\\1\end{pmatrix}\right|^2 = |c_2|^2$$

.

Dans ce cas précis, comme rien ne privilégie une orientation particulière du spin de la particule entrante, on a, par symétrie, $|c_1|^2 = |c_2|^2 = 1/2$, et ces deux probabilités sont égales à 1/2. A l'issue de cette mesure, l'électron bascule dans celui des états propres révélé par la mesure, soit,

$$|\text{out}\rangle = |z+\rangle \qquad \text{ou} \qquad |\text{out}\rangle = |z-\rangle .$$

On dit que la mesure a eu pour effet de préparer l'électron dans un état de spin parfaitement défini. Toute mesure réitérée de M_z ne peut que confirmer la valeur déjà trouvée de même que la projection du vecteur d'état.

2) Voyons à présent ce qui se passe si l'électron, préparé dans l'état, $|z+\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, est analysé par un deuxième appareil de Stern-Gerlach tourné d'un angle, θ, autour de Oy dont on rappelle que l'opérateur associé s'écrit :

$$\mathbf{M}_\theta = \frac{1}{2}\mu_B\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}$$

Les valeurs propres n'ont pas changé, elles valent toujours, $\lambda_1 = \mu_B/2$ ou $\lambda_2 = -\mu_B/2$, mais les vecteurs propres ont changé :

$$|v_1\rangle = R^{-1}_{y,\theta}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{pmatrix} \qquad \text{et} \qquad |v_2\rangle = R^{-1}_{y,\theta}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}-\sin(\theta/2)\\ \cos(\theta/2)\end{pmatrix}.$$

A l'issue de cette mesure, l'électron bascule dans l'état propre révélé par la mesure, soit,

$$|\text{out}\rangle = |v_1\rangle \qquad \text{ou} \qquad |\text{out}\rangle = |v_2\rangle .$$

Les valeurs propres λ_1 (resp. λ_2) ne sont plus équiprobables. Le calcul donne et la mesure confirme :

$$p[\lambda = +(1/2)\mu_0] = \left|\langle z+|v_1\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}(1\ \ 0)\begin{pmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{pmatrix}\right|^2 = \cos^2(\theta/2)$$

$$p[\lambda = -(1/2)\mu_0] = \left|\langle z+|v_2\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}(1\ \ 0)\begin{pmatrix}-\sin(\theta/2)\\ \cos(\theta/2)\end{pmatrix}\right|^2 = \sin^2(\theta/2)$$

.

On note que seuls deux cas mènent à une certitude : si $\theta = 0$, le deuxième appareil confirme le filtrage opéré par le premier tandis que si $\theta = \pi$, la particule préparée dans l'état de moment magnétique, $+\mu_B$, se retrouve assez naturellement dans l'état , $-\mu_B$. Dans tous les autres cas, la composante selon Oz est irrémédiablement perdue en échange de celle selon le nouvel axe. Nous verrons que ceci est en rapport direct avec le principe d'incertitude : de fait les opérateurs, M_z et M_θ, ne commutent pas sauf si $\theta = 0$ ou π.

6) Principe d'évolution. Alors que les opérateurs qui correspondent à des grandeurs observables sont hermitiens, $H = \tilde{H}^*$, ce qui garantit le caractère réel des valeurs propres, ceux qui font évoluer la fonction d'onde sont unitaires, $U^{-1} = \tilde{U}^*$, ce qui préserve la norme unitaire du vecteur d'état. Il existe un lien étroit entre ces deux types d'opérateurs : tout opérateur unitaire peut effectivement s'écrire comme l'exponentielle imaginaire d'un opérateur hermitien :

$$U = \exp[-iH].$$

Le vecteur d'état d'un système évolue en respectant l'équation de Schrödinger :

$$i\hbar\partial_t|\Psi\rangle = H|\Psi\rangle,$$

dont la solution peut s'écrire, dans les cas fréquents où le hamiltonien, H, ne dépend pas du temps :

$$|\Psi(t)\rangle = U(t)|\Psi(0)\rangle = \exp[-\frac{i}{\hbar}Ht]|\Psi(0)\rangle.$$

L'opérateur d'évolution U(t) étant unitaire, la transformation qu'il représente est nécessairement réversible : elle est en effet invertible, $U(t)^{-1}=U(-t)$, et en préservant la norme, elle prévient toute forme de dissipation. Dans cette formule, l'exponentiation de l'opérateur H peut être comprise comme équivalente au développement en série classique ou encore sous la forme spectrale :

$$\exp[-\frac{i}{\hbar}Ht] = \sum_i \exp[-\frac{i}{\hbar}\varepsilon_i t]|\psi_i\rangle\langle\psi_i|,$$

où l'on voit apparaître, en exposant, les valeurs propres de H.

Exemple : on agit sur une particule porteuse d'un moment magnétique en la soumettant à une induction magnétique extérieure constante, $\vec{B}$. Le hamiltonien correspondant s'écrit, dans la base, $(|z+\rangle, |z-\rangle)$:

$$H = -\vec{\mathbf{M}} \cdot \vec{B} = -\frac{\mu_B}{2}\begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix}$$

Cet opérateur jouit de propriétés algébriques remarquables, en particulier ($B^2 = B_x^2 + B_y^2 + B_z^2$) :

$$H^2 = (-\frac{\mu_B}{2})^2 B^2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

d'où il résulte que l'opérateur unitaire qui fait évoluer le vecteur d'état s'écrit :

$$U(t) = \exp[-\frac{i}{\hbar}Ht] = \begin{pmatrix} \cos[\frac{\mu_B B}{2\hbar}t] + i\frac{B_z}{B}\sin[\frac{\mu_B B}{2\hbar}t] & \frac{iB_x + B_y}{B}\sin[\frac{\mu_B B}{2\hbar}t] \\ \frac{iB_x - B_y}{B}\sin[\frac{\mu_B B}{2\hbar}t] & \cos[\frac{\mu_B B}{2\hbar}t] - i\frac{B_z}{B}\sin[\frac{\mu_B B}{2\hbar}t] \end{pmatrix}.$$

Par exemple, un électron préparé dans l'état, $|z+\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, et soumis à une induction constante, $\vec{B}$, évolue comme suit :

$$U|0\rangle = \exp[-\frac{i}{\hbar}Ht]|0\rangle = \left(\cos[\frac{\mu_0 B}{2\hbar}t] + i\frac{B_z}{B}\sin[\frac{\mu_0 B}{2\hbar}t]\right)|0\rangle + \left(\frac{iB_x - B_y}{B}\sin[\frac{\mu_0 B}{2\hbar}t]\right)|1\rangle.$$

Deux cas particuliers valent le détour :

- si l'induction est parallèle à Oz, on trouve :

$$U|0\rangle = \exp[i\frac{\mu_0 B_z}{2\hbar}t]|0\rangle,$$

d'où on conclut que rien d'observable ne se passe du fait que le vecteur d'état est simplement multipliée par une phase inessentielle.

- si l'induction est parallèle à Ox, on trouve :

$$U|0\rangle = \cos[\frac{\mu_0 B_x}{2\hbar}t]|0\rangle + i\sin[\frac{\mu_0 B_x}{2\hbar}t]|1\rangle$$

et on voit que, dès que l'induction cesse d'être parallèle à l'axe qui a servi à préparer l'électron, celui-ci entre dans un état de superposition variable au cours du temps : le filtrage initial, selon $|z+\rangle = |0\rangle$, est détruit.

Le principe et les relations d'incertitude.

Les principes qui précèdent permettent de prédire le résultat de mesures successives de plusieurs propriétés d'une même particule, disons deux pour ne pas compliquer, X et Y. Deux cas sont possibles :

- si les opérateurs associés à chacune d'elles commutent, on a la certitude de pouvoir écrire, en permanence, le vecteur d'état dans le sous-espace commun des vecteurs propres aux deux opérateurs. Il en résulte que l'ont peut faire se succéder plusieurs fois ces mesures dans l'ordre que l'on veut, on trouvera toujours les deux mêmes valeurs, x pour X et y pour Y. On exprime souvent cette conclusion en disant que les deux grandeurs, X et Y, sont simultanément mesurables, ce qui n'est qu'une façon de parler car rien n'exige, dans les faits, que les mesures expérimentales soient réellement faites « simultanément ».

- les choses changent radicalement si les opérateurs associés ne commutent pas. Si on mesure successivement, disons X puis Y puis à nouveau X, on ne retrouvera pas nécessairement la valeur, x, trouvée en premier lieu. En effet, si la première mesure prépare la particule dans l'état x, la deuxième mesure détruit cette préparation du fait qu'elle projette le vecteur d'état sur un sous-espace étranger au sous-espace propre de X. C'est d'ailleurs ce qu'on avait déjà observé lors de l'alignement en série de trois analyseurs de Stern-Gerlach selon Oz, Ox et Oz dans cet ordre.

Lorsque deux grandeurs ne sont pas simultanément mesurables, cela est dû au fait que la mesure de l'une perturbe dramatiquement l'autre. Si on tente malgré tout d'effectuer les mesures on obtiendra des valeurs réparties au hasard dans le spectre des valeurs propres autorisées. Si on répète la manœuvre un grand nombre de fois sur des échantillons issus d'une même source, on verra ces mesures se répartir autour de valeurs moyennes avec une dispersion statistique que le principe d'incertitude se propose d'estimer. Une différence importante apparaît, à ce stade, selon que les opérateurs, X et Y, sont continus ou discrets.

Opérateurs continus qui ne commutent pas. L'exemple classique est celui de la position, x, et de la quantité de mouvement associée, p_x. On a en effet,

$$[x, p_x] = [x, -i\hbar\partial_x] = i\hbar .$$

Il s'avère qu'il est impossible de mesurer avec une précision infinie à la fois x et p_x : les relations d'incertitude fixent une limite infranchissable quelles que soient les ressources expérimentales déployées. Le raisonnement se fait classiquement comme suit : imaginons que l'on prépare 2N particules dans l'état $|\psi(x)\rangle$. On mesure, dans la même configuration expérimentale, la position de N d'entre elles et la quantité de mouvement des N autres. On va s'intéresser aux dispersions des valeurs trouvées autour des moyennes respectives.

Rappelons, tout d'abord, que les probabilités que la position, x, (resp. la quantité de mouvement, p_x) d'une particule occupe l'intervalle (x, x+dx) (resp. (p_x, p_x+dp_x) valent respectivement :

$$dP(x) = |\psi(x)|^2 dx \qquad \text{et} \qquad dP(p_x) = |\Phi(p_x)|^2 dp_x ,$$

où Φ et ψ sont les transformées de Fourier réciproques :

$$\Phi(p_x) = \frac{1}{\sqrt{2\pi\hbar}} \int_{-\infty}^{+\infty} \exp[\frac{i}{\hbar} x p_x] \psi(x) dx \qquad \Leftrightarrow \qquad \psi(x) = \frac{1}{\sqrt{2\pi\hbar}} \int_{-\infty}^{+\infty} \exp[-\frac{i}{\hbar} x p_x] \Phi(p_x) dp_x$$

Selon les théories statistiques en vigueur, on estime la dispersion des positions, x, (resp. des quantités de mouvement, p_x) autour de la moyenne, $\langle x \rangle$, (resp. $\langle p_x \rangle$) par la variance, définie comme suit (Ψ et Φ sont supposées normées dans L_2) :

$$V_{\psi(x)} = \int_{-\infty}^{+\infty} (x - \langle x \rangle)^2 |\psi(x)|^2 dx \qquad \text{et} \qquad V_{\Phi(p_x)} = \int_{-\infty}^{+\infty} (p_x - \langle p_x \rangle)^2 |\Phi(p_x)|^2 dp_x$$

Cette variance est sensée quantifier l'étalement de la fonction ψ (resp. de la fonction Φ) qui est un obstacle naturel à une mesure précise de la position (resp. de la quantité de mouvement) de la particule. Dans le cas d'une mesure individuelle, x, par exemple, on pourrait toujours imaginer raffiner le dispositif expérimental, par exemple en utilisant une fente qui réduirait l'étalement de $\Psi(x)$ mais il en résulterait un étalement accru de $\Phi(p_x)$. C'est la conséquence, physiquement, du phénomène de diffraction lors du passage de la particule au travers de la fente et, mathématiquement, d'un théorème d'analyse qui interdit de concentrer autour d'un point à la fois une fonction et sa transformée de Fourier. Plus précisément, ce théorème affirme que le produit de leurs variances est borné inférieurement par une constante positive :

$$V_\psi \times V_\Phi \geq \frac{\hbar^2}{4}.$$

Cette relation porte le nom de relation d'incertitude d'Heisenberg pour le couple des variables x et p_x. La question se pose du caractère optimal de cette relation. On voit bien qu'elle instaure une limite conceptuelle à la mesure simultanée de grandeurs continues qui ne commutent pas mais le signe d'inégalité fait précisément craindre que ce résultat soit trop tolérant. Il l'est en effet. Pour le voir nous considérons deux cas extrêmes.

Considérons tout d'abord la fonction gaussienne, centrée sur l'origine pour simplifier, et sa transformée de Fourier, toutes deux normalisées dans L_2 :

$$\psi(x) = \frac{1}{\sqrt{\sigma\sqrt{\pi}}} \exp[-\frac{x^2}{2\sigma^2}] \qquad \Leftrightarrow \qquad \Phi(p_x) = \sqrt{\frac{\sigma}{\hbar\sqrt{\pi}}} \exp[-\frac{\sigma^2 p_x^2}{2\hbar^2}].$$

Le calcul des variances se fait exactement. On trouve respectivement, $V_\psi = \frac{\sigma^2}{2}$ et $V_\Phi = \frac{\hbar^2}{2\sigma^2}$, d'où on voit que le produit des variances vaut : $V_\psi \times V_\Phi = \frac{\hbar^2}{4}$. De toute évidence, il n'y a pas moyen de faire mieux : la relation d'incertitude est optimale dans ce cas.

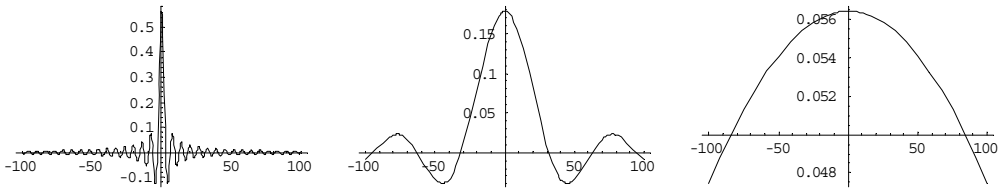
Cependant, il n'est pas difficile de trouver un exemple bien moins favorable, à tel point que l'une des variances n'est même pas définie ! Considérons, en effet, la fonction caractéristique de l'intervalle [-a,a], normalisée dans L_2,

$$\psi(x) = \frac{1}{\sqrt{2a}}\delta_{[-a,a]}.$$

Cette fonction n'a rien d'extravagante puisqu'elle correspond au passage équiprobable d'une particule en tout point d'une fente de largeur 2a. Sa transformée de Fourier, normalisée dans L_2, se calcule facilement :

$$\psi(x) = \frac{1}{\sqrt{2a}}\delta_{[-a,a]} \qquad \Leftrightarrow \qquad \Phi(p_x) = \sqrt{\frac{\hbar}{\pi a}}\,\frac{\sin(ap_x/\hbar)}{p_x}.$$

Les figures qui suivent montrent à quel point la transformée de Fourier, Φ, s'élargit à mesure que a rapetisse (successivement a = 1 , 1/10, 1/100, dans un système d'unités où $\hbar = 1$) :



La variance, V, de Ψ est parfaitement définie :

$$V_{\psi(x)} = \int_{-\infty}^{+\infty}(x - \langle x\rangle)^2 |\psi(x)|^2\,dx = \frac{a^2}{3}$$

mais ce n'est malheureusement pas le cas de sa transformée de Fourier :

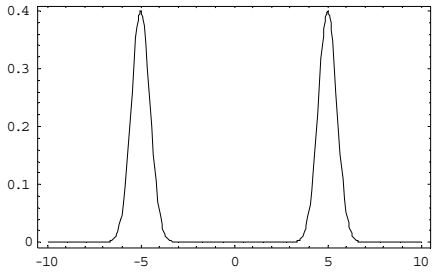
$$V_{\Phi(p_x)} = \int_{-\infty}^{+\infty}(p_x - \langle p_x\rangle)^2 |\Phi(p_x)|^2\,dp_x = \infty \ !$$

On a certes toujours l'inégalité, $V_\psi \times V_\Phi \geq \frac{\hbar^2}{4}$, mais elle a perdu tout intérêt. Le nœud de l'affaire réside apparemment dans la définition de la variance : une fonction de carré intégrable ne l'est plus forcément, à l'infini, lorsqu'on la multiplie par un facteur quadratique.

Mais on peut faire une autre objection à la notion de variance qui est celle de ne pas décrire correctement l'étalement d'une fonction qui présente plusieurs pics d'intensités. Considérons, en effet, la fonction suivante qui présente deux pics d'intensité espacés :

$$\psi(x) = \lambda\left(\exp[-(x-5)^2] + \exp[-(x+5)^2]\right),$$

où la constante, $\lambda = \frac{e^{25}}{\sqrt[4]{2\pi}\sqrt{e^{50}+1}}$, garantit la normalisation dans L_2. Voici son graphe :



La variance de cette fonction et de sa transformée de Fourier valent respectivement :

$$V_\psi = \frac{1+101e^{50}}{4+4e^{50}} \text{ et } V_\Phi = \hbar^2 \frac{e^{50}-99}{e^{50}+1}.$$

Leur produit, $25.25\hbar^2$, excède largement le minimum annoncé, $0.25\hbar^2$. C'est la conséquence d'une définition qui privilégie l'écart à la moyenne et qui ignore de fait la position des pics.

Une définition plus fidèle de l'étalement d'une fonction trouve son origine dans la théorie de Shannon. On définit l'entropie d'une fonction, Ψ, normalisée dans L_2 par la formule :

$$S_{\psi(x)} = -\int_{-\infty}^{+\infty} |\psi(x)|^2 \ell n(|\psi(x)|^2) dx$$

où la base utilisée pour le logarithme n'a pas vraiment d'importance. On commence par noter que cette définition ne fait aucune différence avec la variance si Ψ est simplement gaussienne, $\psi(x) = \frac{1}{\sqrt{\sigma\sqrt{\pi}}} \exp[-\frac{(x-\langle x\rangle)^2}{2\sigma^2}]$. Par contre, elle reste parfaitement définie dans le cas de la fonction rectangulaire, $\psi(x) = \frac{1}{\sqrt{2a}} \delta_{[-a,a]}$. De plus, elle rend beaucoup mieux compte de la notion d'étalement de la fonction lorsque celle-ci présente plusieurs pics d'intensité. Dans l'exemple traité précédemment, $\psi(x) = \lambda\left(\exp[-(x-5)^2] + \exp[-(x+5)^2]\right)$, chaque gaussienne présente une variance (ou une entropie puisqu'elle sont égales dans ce cas), valant 1/4. La variance de la superposition des deux vaut 25.25 alors que l'entropie globale vaut 1.41894. Tout cela est inscrit dans une inégalité due à Shannon :

$$S_\psi \le \frac{1}{2} \ell n(2\pi e V_\psi).$$

Un avantage décisif de la notion d'entropie du vecteur d'état résulte de l'inégalité suivante :

$$V_\psi \times V_\Phi \ge \frac{1}{4\pi^2} \exp[2(S_\psi + S_\Phi - 1)] \ge \frac{\hbar^2}{4},$$

dont la partie droite renforce visiblement l'inégalité d'Heisenberg sous la forme équivalente (Ψ et Φ doivent être normalisés dans L_2) :

$S_\psi + S_\Phi \geq \ell n(\pi e\hbar)$.

C'est la version entropique du principe d'incertitude. L'inégalité se transforme encore en égalité dans le cas gaussien mais elle est généralement supérieure à l'inégalité basée sur la variance dans les autres cas. Un autre avantage de cette version provient de ce que la généralisation au cas discret est possible.

Opérateurs discrets qui ne commutent pas. Comme exemple d'opérateurs discrets nous choisissons tout naturellement les opérateurs de spin 1/2. Dans la notation de Dirac, la variance d'un ensemble de mesures relatives à l'opérateur, A, lorsque la particule se trouve dans l'état, $|\psi\rangle$, se note :

$$V_A(|\psi\rangle) = \langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2,$$

et l'inégalité d'Heisenberg relative à tout couple d'opérateurs, A et B, qui ne commutent pas s'écrit classiquement sous la forme, due à Robertson :

$$V_A(|\psi\rangle)V_B(|\psi\rangle) \geq \frac{1}{4}\left|\langle\psi|[A,B]|\psi\rangle\right|^2.$$

Pour la petite histoire, Schrödinger a montré que cette inégalité pouvait être raffinée :

$$V_A(|\psi\rangle)V_B(|\psi\rangle) \geq \frac{1}{4}\left|\langle\psi|[A,B]|\psi\rangle\right|^2 + \frac{1}{4}\left|\langle\psi|\{A-\langle\psi|A|\psi\rangle, B-\langle\psi|B|\psi\rangle\}|\psi\rangle\right|^2,$$

où {A,B}=AB+BA.

Dans le cas du spin 1/2, ces deux variantes mènent au même résultat trivial :

$$V_{S_z}(|\psi\rangle)V_{S_x}(|\psi\rangle) \geq \frac{\hbar^2}{4}\left|\langle\psi|S_y|\psi\rangle\right|^2 = 0\ .$$

De fait, si on analyse un flux de 2N particules n'ayant subi aucune préparation préalable, on trouve une dispersion des mesures réparties aléatoirement entre les valeurs, $s_x = \pm\hbar/2$, pour N particules analysées selon Oz (idem pour les N autres, analysées selon Ox) et le produit des variances vaut $\hbar^4/16$. Il ne nous avance guère d'apprendre que cette constante est positive !

La version entropique du principe d'incertitude est bien meilleure. En guise d'illustration, nous considérons l'espace de Hilbert associé à une particule de spin 1/2 dans l'état, $|\psi\rangle$. Notons $|0\rangle$ et $|1\rangle$ les vecteurs de base de cet espace. On définit l'entropie de la particule dans cet état, $|\psi\rangle$, comme suit :

$$S = -\sum_i \left|\langle\psi|i\rangle\right|^2 \ell n\left|\langle\psi|i\rangle\right|^2 = -\left(\left|\langle\psi|0\rangle\right|^2 \ell n\left|\langle\psi|0\rangle\right|^2 - \left|\langle\psi|1\rangle\right|^2 \ell n\left|\langle\psi|1\rangle\right|^2\right).$$

On voit qu'une particule préparée dans un état de base, $|0\rangle$ ou $|1\rangle$, possède une entropie nulle. Si, pour une raison quelconque, on perd le contrôle de cet état et que la particule entre dans un état de superposition du type, $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$, l'entropie augmente à la valeur,

$$S = -\left(|c_1|^2 \ell n(|c_1|^2) + |c_2|^2 \ell n(|c_2|^2)\right) \qquad (|c_1|^2 + |c_2|^2 = 1)$$

dont la valeur maximum (= 1 bit) est atteinte lorsque, $|c_1|^2 = |c_2|^2 = 1/2$. Inversement, lorsqu'une mesure fait passer de l'état de superposition vers un des états de base, l'entropie de la particule diminue de 1 bit. Toutefois, la trace objective que la mesure laisse subsister au niveau de l'appareil de mesure compense cette diminution d'entropie par une augmentation au moins équivalente. Au total, et dans tous les cas, l'entropie de l'univers ne diminue jamais.

Revenons au principe d'incertitude dans le cas discret. Si on tente une mesure simultanée de deux grandeurs, A et B, on a la version entropique suivante. Soit, $|a_0\rangle$ et $|a_1\rangle$, d'une part et, $|b_0\rangle$ et $|b_1\rangle$, d'autre part, les vecteurs propres des opérateurs A et B, on peut démontrer la double inégalité entropique suivante :

$$2 \geq S_A(|\psi\rangle) + S_B(|\psi\rangle) \geq -2\ell g \sup_{i,j} |\langle a_i | b_j \rangle| \quad \text{(bits)} \qquad (= -2\ell n \sup_{i,j} |\langle a_i | b_j \rangle| \quad \text{(nats)}).$$

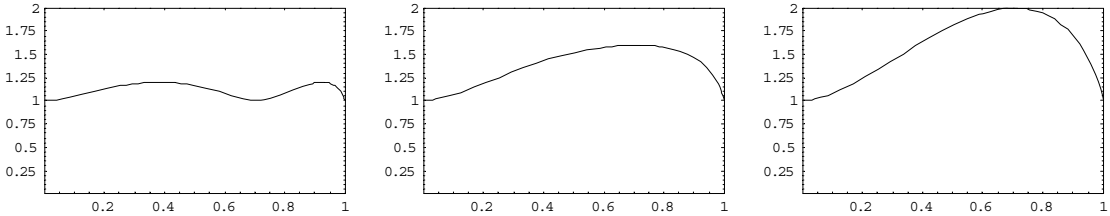
Exemple 1 : soit les opérateurs, S_z =A et S_x =B, qui ne commutent pas. On calcule sans peine leurs vecteurs propres :

$$|a_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |a_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |b_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad |b_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

d'où la relation d'incertitude,

$$2 \geq S_{S_z}(|\psi\rangle) + S_{S_x}(|\psi\rangle) \geq 1 \quad \text{(bit)} \qquad (= -2\ell n \frac{1}{\sqrt{2}} \quad \text{(nats)}).$$

Voyons, par un calcul direct, ce que donne cette relation sur l'état, $|\psi\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \gamma_1 \\ e^{i\varphi}\gamma_2 \end{pmatrix}$, où les c_i peuvent être complexes mais pas les $\gamma_i, (\gamma_1^2 + \gamma_2^2 = 1)$. On trouve les graphes suivants de S_{tot} en fonction de γ_1 variant entre 0 et 1, pour quelques déphasages simples, respectivement, $\varphi = 0, \pi/4, \pi/2$:



On constate que l'entropie totale est toujours supérieure à 1 bit et qu'elle n'excède évidemment jamais 2 bits. Le minimum entropique, 1bit, correspond aux états propres de l'un ou l'autre des opérateurs, A ou B et le maximum absolu, 2 bits, est atteint pour l'état, $|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm i \end{pmatrix}$.

Exemple 2 : soit les opérateurs, S_z = A et S^2 = B, qui commutent. On calcule sans peine les vecteurs propres suivants :

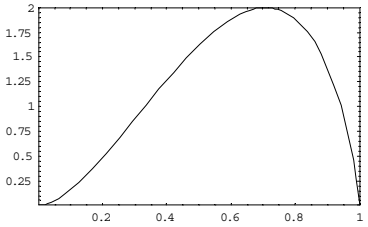
$$|a_0\rangle = |b_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |a_1\rangle = |b_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

d'où la relation d'incertitude,

$$2 \geq S_{S_z}(|\psi\rangle) + S_{S_x}(|\psi\rangle) \geq 0 .$$

De fait dans le cas des opérateurs qui commutent on trouve, tous calculs faits :

$S = -\left(|c_1|^2 \ell n(|c_1|^2) + |c_2|^2 \ell n(|c_2|^2)\right)$ (nats), dont le graphe s'étale entre 0 et 2 bits.



Annexe 1 : Opérateurs quantiques.

1.1. Opérateurs continus.

Il est inscrit dans les principes de la théorie quantique qu'un opérateur soit associé à toute grandeur physique mesurable. C'est en partant d'analogies classiques, qu'on a historiquement dégagé les opérateurs les plus courants, ceux qui correspondent à l'énergie, à la position, à la quantité de mouvement et au moment cinétique. Les exposés traditionnels continuent de s'appuyer sur ces analogies pour justifier l'écriture des opérateurs quantiques. Sauf à imaginer se donner bonne conscience en procédant de cette façon, nous pensons que cela n'a aucun sens de justifier les options d'une théorie à partir d'une autre que l'on veut précisément supplanter. Il est plus radical de ne pas s'encombrer de telles analogies : la mécanique quantique précède la mécanique classique et il n'y a pas lieu de tenter de justifier la première à partir de la seconde. Il est plus sain de poser, une fois pour toutes, les bases nécessaires à la théorie quantique puis d'en tirer ultérieurement les conséquences au niveau de l'approximation classique. Quoi qu'il en soit, voici le détail de l'écriture des opérateurs les plus courants en commençant par ceux qui concernent les variables continues de position et de quantité de mouvement :

$$(x, y, z) \Rightarrow (x, y, z)$$
$$(p_x, p_y, p_z) \Rightarrow -i\hbar(\partial_x, \partial_y, \partial_z) .$$

Il est bien connu que tous ces opérateurs commutent sauf, x et p_x, y et p_y, et, z et p_z. Le temps est un paramètre et l'opérateur énergie lui est associé sous la forme :

$$H \Rightarrow i\hbar\partial_t .$$

Les opérateurs associés au moment angulaire orbital se notent, assez naturellement :

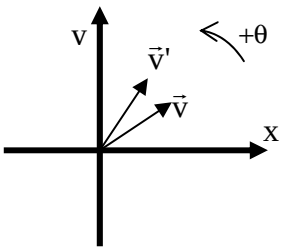
$$(L_x, L_y, L_z) \Rightarrow -i\hbar(y\partial_z - z\partial_y, z\partial_x - x\partial_z, x\partial_y - y\partial_x) .$$

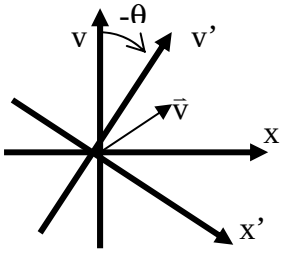
On rappelle qu'ils obéissent aux relations de commutation :

$$\left[L_x, L_y\right] = i\hbar L_z \qquad \left[L_y, L_z\right] = i\hbar L_x \qquad \left[L_z, L_x\right] = i\hbar L_y$$

1.2. Changements de repère applicables aux opérateurs continus.

Il arrive que l'on soit amené à travailler dans un référentiel différent du référentiel original, Oxyz. Nous envisagerons deux cas : le nouveau repère est obtenu par translation ou par rotation de l'ancien. Dans les deux cas le problème posé est le suivant : comment traduire les vecteurs d'état et les opérateurs dans le nouveau repère ? La solution à ce problème est bien connue : elle passe par l'introduction d'un opérateur supplémentaire, R, dit de changement de repère. Dans l'espace euclidien habituel, tout est simple sauf à prendre soin des signes. Les deux descriptions qui suivent sont équivalentes : soit on fait tourner un vecteur dans un repère fixe, d'un angle, θ, autour de l'axe Oz, pour faire simple, puis on cherche ses nouvelles composantes soit on fixe le vecteur et on fait tourner les axes en sens inverse.





Les lois de transformation cherchées se notent avec l'aide de la matrice de rotation, $R_{z,-\theta}$, des axes selon l'angle, $-\theta$:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \qquad \Leftrightarrow \qquad \vec{v}' = R_{z,-\theta}\vec{v} = R_{z,\theta}^{-1}\vec{v}\,.$$

Cette règle se généralise aux espaces de Hilbert et on a que tout vecteur d'état subit la matrice inverse de celles subies par les axes :

$$|v'\rangle = R^{-1}|v\rangle\,.$$

On en déduit la loi de transformation qui concerne les opérateurs :

$$\hat{O}' = R^{-1}\hat{O}R$$

et on vérifie que ces lois préservent, comme il se doit, les valeurs propres des opérateurs :

$$\hat{O}'|v'\rangle = \lambda|v'\rangle \qquad \Leftrightarrow \qquad \hat{O}|v\rangle = \lambda|v\rangle\,.$$

Reste à trouver l'expression des opérateurs de translation et de rotation. Bien que nous n'en fassions aucun usage, l'opérateur de translation d'une distance, ℓ, selon l'axe Ox, est suffisamment simple pour comprendre comment il opère. On l'écrit :

$$T_{x,\ell} = \exp[i\frac{\ell p_x}{\hbar}] = \exp[\ell\partial_x]\,.$$

Il suffit de l'appliquer à une fonction quelconque dépendante de x pour vérifier, par une simple application de la formule de Taylor, qu'il a bien pour effet de translater la fonction :

$$T_{x,\ell} f(x) = f(x+\ell)\,.$$

Les opérateurs de rotations autour des axes de référence se construisent et s'appliquent en suivant le même principe :

$$R_{x,\theta} = \exp[i\frac{\theta L_x}{\hbar}] \qquad R_{y,\theta} = \exp[i\frac{\theta L_y}{\hbar}] \qquad R_{z,\theta} = \exp[i\frac{\theta L_z}{\hbar}]\,.$$

Un calcul facile mais ennuyeux indique que l'on a effectivement :

$$R_{z,\theta} f(x,y,z) = R_{z,\theta} f(\vec{r}) = f(x\cos\theta - y\sin\theta, -x\sin\theta + y\cos\theta, z).$$

2.1. Opérateurs discrets.

Les opérateurs continus ne sont pas intéressants pour le développement de la théorie quantique de l'information. Par contre les opérateurs discrets, associés aux degrés de liberté internes de spin, sont intéressants. Le spin ne possède pas d'analogue classique mais on pose que ses composantes obéissent aux mêmes relations de commutations que L :

$$[S_x, S_y] = i\hbar S_z \qquad [S_y, S_z] = i\hbar S_x \qquad [S_z, S_x] = i\hbar S_y .$$

La partie du vecteur d'état qui décrit ce spin appartient à un espace de Hilbert de dimension finie, (2s+1) pour les particules de spin s, dont il est facile de trouver une représentation matricielle. Pour les particules de spin ½, on trouve les matrices 2x2, dites de Pauli,

$$S_x^{(2)} = \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad S_y^{(2)} = \frac{\hbar}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad S_z^{(2)} = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

et pour celles de spin 1, on trouve de même,

$$S_x^{(3)} = \frac{\hbar}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad S_y^{(3)} = \frac{\hbar}{\sqrt{2}}\begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix} \qquad S_z^{(3)} = \hbar\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Chaque état de spin, s, est donc décrit par un vecteur d'état à 2s+1 composantes et ce sont précisément ces états discrets qui offrent un modèle possible pour le qubit.

2.2. Changements de repère applicables aux opérateurs discrets.

On pose que les opérateurs de rotation qui transforment les opérateurs discrets lors d'un changement de repère sont semblables à ceux qui transforment les opérateurs continus sauf à remplacer les composantes de L par celles de S. Voici les représentations matricielles des opérateurs de rotation valables pour le spin 1/2 :

$$R_{x,\theta}^{(2)} = \exp[(i/\hbar)\theta S_x^{(2)}] = \begin{pmatrix} \cos(\theta/2) & i\sin(\theta/2) \\ i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

$$R_{y,\theta}^{(2)} = \exp[(i/\hbar)\theta S_y^{(2)}] = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

$$R_{z,\theta}^{(2)} = \exp[(i/\hbar)\theta S_z^{(2)}] = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}.$$

L'exemple suivant est particulièrement important puisqu'il concerne l'analyseur de Stern-Gerlach. L'opérateur associé au moment magnétique selon Oz, $\mathtt{M}_z$, d'une particule de spin 1/2 possède la représentation matricielle diagonale suivante (μ_B est le magnéton de Bohr) :

$$\mathtt{M}_z = \mu_B S_z^{(2)} = \mu_B \begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix}.$$

Si on décide de tourner l'analyseur de Stern-Gerlach d'un angle θ par rapport à Oy dans le sens direct, l'opérateur associé à la mesure du moment magnétique de la particule de spin 1/2 selon un la nouvelle direction qu'il définit s'obtient en appliquant l'opérateur de changement de repère :

$$\mathtt{M}_\theta = R_{y,\theta}^{-1} \mu_B \begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix} R_{y,\theta} = \frac{1}{2}\mu_B \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

On observe, en passant, que cette relation aurait tout aussi bien pu s'écrire :

$$\mathbf{M}_\theta = \mathbf{M}_z \cos\theta - \mathbf{M}_x \sin\theta.$$

On reconnaît la loi de transformation de la composantes, z, d'un vecteur lors d'une rotation des axes d'angle, -θ, par rapport à Oy. En particulier, si θ = -π/2, on retrouve : $\mathtt{M}_\theta = \mathtt{M}_x$.

Les valeurs propres de $\mathtt{M}_\theta$ valent toujours, $\lambda_1 = \mu_B/2$ ou $\lambda_2 = -\mu_B/2$, et les vecteurs propres se calculent directement ou en appliquant la loi de transformation pour les vecteurs d'états :

$$|v_1\rangle = R_{y,\theta}^{-1}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix} \qquad \text{et} \qquad |v_2\rangle = R_{y,\theta}^{-1}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix}.$$

Les projecteurs, P_i, associés à chacune des valeurs propres s'écrivent :

$$\hat{P}_1 = |v_1\rangle\langle v_1| = \begin{pmatrix} \cos^2(\theta/2) & \sin(\theta/2)\cos(\theta/2) \\ \sin(\theta/2)\cos(\theta/2) & \sin^2(\theta/2) \end{pmatrix},$$

$$\hat{P}_2 = |v_2\rangle\langle v_2| = \begin{pmatrix} \sin^2(\theta/2) & \sin(\theta/2)\cos(\theta/2) \\ \sin(\theta/2)\cos(\theta/2) & \cos^2(\theta/2) \end{pmatrix}.$$

Voici, à présent, les représentations matricielles des opérateurs de rotation, pour le spin 1 :

$$R_{x,\theta}^{(3)} = \exp[(i/\hbar)\theta S_x] = \begin{pmatrix} \cos^2(\theta/2) & i\sin\theta/\sqrt{2} & \sin^2(\theta/2) \\ i\sin\theta/\sqrt{2} & \cos\theta & i\sin\theta/\sqrt{2} \\ \sin^2(\theta/2) & i\sin\theta/\sqrt{2} & \cos^2(\theta/2) \end{pmatrix},$$

$$R^{(3)}_{y,\theta} = \exp[(i/\hbar)\theta S_y] = \begin{pmatrix} \cos^2(\theta/2) & \sin\theta/\sqrt{2} & \sin^2(\theta/2) \\ -\sin\theta/\sqrt{2} & \cos\theta & \sin\theta/\sqrt{2} \\ \sin^2(\theta/2) & -\sin\theta/\sqrt{2} & \cos^2(\theta/2) \end{pmatrix},$$

$$R^{(3)}_{z,\theta} = \exp[(i/\hbar)\theta S_z] = \begin{pmatrix} e^{i\theta} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{-i\theta} \end{pmatrix}.$$

Ici, s=1, et l'opérateur associé au moment magnétique selon Oz, M_z, possède la représentation matricielles diagonale suivante :

$$M_z = \mu_B S^{(3)}_z = \mu_B \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Si on décide de tourner l'analyseur de Stern-Gerlach d'un angle θ par rapport à Oy dans le sens direct, l'opérateur associé à la mesure du moment magnétique de la particule de spin 1 selon un la nouvelle direction qu'il définit s'obtient en appliquant l'opérateur de changement de repère :

$$M_\theta = R^{-1}_{y,\theta}\mu_B \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} R_{y,\theta} = \frac{1}{2}\mu_B \begin{pmatrix} \cos\theta & \frac{\sin\theta}{\sqrt{2}} & 0 \\ \frac{\sin\theta}{\sqrt{2}} & 0 & \frac{\sin\theta}{\sqrt{2}} \\ 0 & \frac{\sin\theta}{\sqrt{2}} & -\cos\theta \end{pmatrix}.$$

On a encore :

$$\mathbf{M}_\theta = \mathbf{M}_z \cos\theta - \mathbf{M}_x \sin\theta = \mathbf{M}_z \cos(-\theta) + \mathbf{M}_x \sin(-\theta).$$

Les valeurs propres de M_θ valent toujours, $\lambda_1 = \mu_B$, $\lambda_2 = 0$ ou $\lambda_3 = -\mu_B$, et les vecteurs propres se calculent, à nouveau, directement ou en appliquant la loi de transformation pour les vecteurs d'états :

$$|v_1\rangle = R^{-1}_{y,\theta}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos^2(\theta/2) \\ \frac{\sin\theta}{\sqrt{2}} \\ \sin^2(\theta/2) \end{pmatrix} \qquad |v_2\rangle = R^{-1}_{y,\theta}\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -\frac{\sin\theta}{\sqrt{2}} \\ \cos\theta \\ \frac{\sin\theta}{\sqrt{2}} \end{pmatrix} \qquad |v_3\rangle = R^{-1}_{y,\theta}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \sin^2(\theta/2) \\ -\frac{\sin\theta}{\sqrt{2}} \\ \cos^2(\theta/2) \end{pmatrix}$$

A condition de disposer d'assez de place, les projecteurs, P_i, associés à chacune des valeurs propres s'écriraient :

$$\hat{P}_i = |v_i\rangle\langle v_i| \qquad (i = 1,2,3).$$

Annexe 2 : Equations d'onde.

Les calculs explicites de cet appendice sont effectués en annexe dans le cadre d'une session Mathematica.

Ouvrons une parenthèse pour évoquer l'équation d'évolution des particules spinales. Toute particule possède des degrés de liberté externes (position, quantité de mouvement, etc) et internes (spin). Une équation acceptable doit rencontrer un certain nombre d'exigences :

- être du premier ordre,
- être relativiste, c'est-à-dire invariante par rapport à la transformation de Lorentz,
- impliquer l'équation de Klein-Gordon, $\frac{1}{c^2}\partial_t^2\Psi = \nabla^2\Psi - \left(\frac{mc}{\hbar}\right)^2\Psi$,
- permettre la définition d'une densité de probabilité de présence positive et enfin,
- autoriser la définition d'un hamiltonien qui commute avec le moment cinétique total, L_z+S_z.

Dirac fut le premier à comprendre que la solution à ce problème passait par la démultiplication du nombre des composantes de la fonction d'onde, typiquement, 4s+2, pour toute particule de spin s. Le hamiltonien s'exprime alors à l'aide de quatre matrices, α_x, α_y, α_z et β, de dimensions (4s+2)x(4s+2) :

$$(\hat{H}\psi =)\quad i\hbar\partial_t\psi = -ic\hbar(\alpha_x\partial_x + \alpha_y\partial_y + \alpha_z\partial_z)\psi + \beta mc^2\psi .$$

On détermine les matrices inconnues en exigeant qu'il existe un opérateur de spin, S_z, tel que H commute avec L_z+S_z. Or on calcule aisément que (cfr annexe) :

$$[H, L_z] = -c\hbar^2\left[\alpha_x\partial_y - \alpha_y\partial_x\right]$$

On doit donc définir S_z en sorte que l'on ait :

$$[H, S_z] = c\hbar^2\left[\alpha_x\partial_y - \alpha_y\partial_x\right].$$

Cela exige que l'on ait simultanément :

$$[\alpha_x, S_z] = -\hbar\alpha_y \qquad [\alpha_y, S_z] = \hbar\alpha_x \qquad [\alpha_z, S_z] = 0 \qquad [\beta, S_z] = 0 .$$

Les trois premières relations suggèrent de calquer les α sur les matrices de spin. Une solution consiste donc à poser :

$$\alpha_{x,y,z} = \begin{pmatrix} \sigma_{x,y,z} & 0 \\ 0 & -\sigma_{x,y,z} \end{pmatrix}, \qquad \beta = \begin{pmatrix} 0 & -\mathrm{Id} \\ -\mathrm{Id} & 0 \end{pmatrix}, \qquad S_{x,y,z} = \hbar\begin{pmatrix} \sigma_{x,y,z} & 0 \\ 0 & \sigma_{x,y,z} \end{pmatrix},$$

où les matrices σ et Id sont respectivement les matrices (2s+1)x(2s+1) de Pauli généralisées et identité. On obtient l'équation d'onde suivante :

$$(\hat{H}\psi =)\quad i\hbar\partial_t\psi = -ic\hbar\begin{pmatrix}\vec{\sigma}\cdot\vec{\nabla} & 0\\ 0 & -\vec{\sigma}\cdot\vec{\nabla}\end{pmatrix}\psi + mc^2\begin{pmatrix}0 & -Id\\ -Id & 0\end{pmatrix}\psi .$$

Il importe d'être conscient qu'il existe en fait une infinité de représentations équivalentes dérivant de celle-ci par n'importe quelle transformation unitaire, U. On a en effet l'équivalence suivante :

$$i\hbar\partial_t\psi = \hat{H}\psi \qquad \Leftrightarrow \qquad i\hbar\partial_t(U^{-1}\psi) = (U^{-1}\hat{H}U)(U^{-1}\psi) .$$

La représentation chirale est particulièrement importante car l'opérateur associé à la composante selon Oz du spin y est naturellement diagonal. On a en effet :

$$S_z = \hbar\begin{pmatrix}\sigma_z & 0\\ 0 & \sigma_z\end{pmatrix}.$$

<u>Particule de spin 1/2.</u>

Dans la représentation chirale, la théorie précédente s'applique, il suffit d'utiliser les matrices simples 2x2 de Pauli et la matrice identité :

$$\sigma_x = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad \sigma_y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \qquad \sigma_z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \qquad Id_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Quant à la fonction d'onde, elle comporte quatre composantes que l'on peut agréablement ranger en deux bispineurs,

$$\Psi_{él} = \begin{pmatrix}\varphi\\ \chi\end{pmatrix}$$

Ces composantes obéissent à deux équations couplées de dimensions deux :

$$i\hbar\partial_t\varphi = -mc^2\chi - i\hbar c\vec{\sigma}.\vec{\nabla}\varphi$$
$$i\hbar\partial_t\chi = -mc^2\varphi + i\hbar c\vec{\sigma}.\vec{\nabla}\chi$$

<u>Particule de spin 1.</u>

Le même schéma s'applique aux particules de spin 1, sauf qu'il faut remplacer les matrices 2x2, σ, de Pauli par les matrices 3x3, correspondantes, déjà rencontrées :

$$\sigma_x = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 0\end{pmatrix} \qquad \sigma_y = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & -i & 0\\ i & 0 & -i\\ 0 & i & 0\end{pmatrix} \qquad \sigma_z = \begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & -1\end{pmatrix} \qquad Id_3 = \begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}$$

Ces formes matricielles correspondent à la représentation chirale puisque σ_z est diagonal. La fonction d'onde comporte cette fois six composantes que l'on peut encore ranger en deux parties,

$$\psi_{spin1} = \begin{pmatrix} \varphi \\ \chi \end{pmatrix}.$$

Elles obéissent encore à deux équations couplées de dimensions trois :

$$\begin{aligned} i\hbar\partial_t\varphi &= -mc^2\chi - i\hbar c\vec{\sigma}.\vec{\nabla}\varphi \\ i\hbar\partial_t\chi &= -mc^2\varphi + i\hbar c\vec{\sigma}.\vec{\nabla}\chi \end{aligned}.$$

Dans le cas particulier mais important du photon, le terme de masse disparaît et ces équations coïncident avec les lois d'Ampère et de Faraday. Il suffit, pour s'en convaincre, de poser que les six composantes de la fonction d'onde sont un mélange convenable des trois composantes des champs électrique et magnétique :

$$\psi_{photon} = \frac{1}{\sqrt{2}} \begin{pmatrix} -(E_x + icB_x) + i(E_y + icB_y) \\ \sqrt{2}(E_z + icB_z) \\ (E_x + icB_x) + i(E_y + icB_y) \\ -(E_x - icB_x) + i(E_y - icB_y) \\ \sqrt{2}(E_z - icB_z) \\ (E_x - icB_x) + i(E_y - icB_y) \end{pmatrix}.$$

On peut simplifier la présentation en travaillant dans une représentation autre que la représentation chirale (cfr annexe). On a alors que la fonction d'onde peut être reliée simplement aux champs classiques sous la forme plus agréable :

$$\Psi_{photon} = \begin{pmatrix} \vec{E} + ic\vec{B} \\ \vec{E} - ic\vec{B} \end{pmatrix}.$$

On remarque que la disparition de la constante de Planck dans l'équation d'évolution du photon résulte de l'absence de masse de celui-ci. Cela explique pourquoi les équations de Maxwell, bien que d'essence classique, prédisent correctement tous les phénomènes optiques tout en s'en tenant à un point de vue ondulatoire. En particulier, la théorie de la polarisation lumineuse se développe indifféremment sur base de l'existence d'un champ électromagnétique transversal ou d'un photon doué d'une hélicité gauche ou droite

Il subsiste deux points à éclaircir. En premier lieu, un lecteur attentif aura remarqué que deux équations de Maxwell manquent à l'appel dans le décompte précédent. La raison en est que, contrairement à ce qui se passe dans le cas du spin 1/2, l'équation valable pour le spin 1,

$$(\hat{H}\psi =) \quad i\hbar\partial_t\psi = -ic\hbar \begin{pmatrix} \vec{\sigma}\cdot\vec{\nabla} & 0 \\ 0 & -\vec{\sigma}\cdot\vec{\nabla} \end{pmatrix} \psi + mc^2 \begin{pmatrix} 0 & -Id \\ -Id & 0 \end{pmatrix} \psi,$$

ne garantit pas automatiquement que ses solutions obéissent à l'équation de Klein-Gordon. Il faut imposer deux conditions supplémentaires qui ne s'expriment simplement que lorsque la masse de la particule vaut zéro, ce qui est heureusement le cas du photon. Dans ce cas précis, les calculs détaillés (cfr annexe) indiquent que ces conditions s'écrivent :

$$\mathrm{div}\vec{E} = 0 \qquad \text{et} \qquad \mathrm{div}\vec{B} = 0\,,$$

et on voit apparaître les deux lois de Gauss.

Enfin, le deuxième point concerne l'absence d'état de spin zéro pour le photon. Les calculs détaillés dans l'annexe montrent qu'une solution de l'équation d'évolution en forme d'onde plane exige l'annulation des composantes longitudinales, E_z et B_z, qui correspondent précisément à l'état de spin S_z nul. Comme une fonction d'onde ne peut jamais être nulle, on en conclut qu'il ne peut exister d'état propre correspondant à la valeur $S_z = 0$.

En résumé, l'inexistence de la composante de spin zéro du photon apparaît indifféremment comme la conséquence de la transversalité obligatoire des champs dans une onde électromagnétique, ou encore des deux lois de Gauss. Ce sont trois manières différentes d'exprimer la même idée en partant de points de vues différents.

Annexe 3 : Le qutrit encodé grâce à une particule de spin 1.

L'expérience de Stern-Gerlach peut être recommencée avec un faisceau de particules chargées de spin 1. Elle révèle trois impacts discrets sur l'écran, qui correspondent à des moments magnétiques $+\mu_B$, 0 et $-\mu_B$. Sur la figure de référence, ils se situeraient en A, B et C.

Cette fois, l'opérateur associé à la grandeur mesurée, $\mathtt{M}_z$, se note, dans la base naturelle :

$$\mathtt{M}_z = \mu_B S_z = \mu_B \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Les valeurs observables sont les valeurs propres, $\lambda_1 = \mu_B$ et $\lambda_2 = 0$ et $\lambda_3 = -\mu_B$, et les vecteurs propres correspondants forment la base orthonormée, que l'on note indifféremment :

$$|v_1\rangle = |z+\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \qquad |v_2\rangle = |z0\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \qquad \text{et} \qquad |v_3\rangle == |z-\rangle = |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Si le faisceau initial se trouve dans l'état de superposition général,

$$|in\rangle = c_1|z+\rangle + c_2|z0\rangle + c_3|z-\rangle,$$

les probabilités qu'une mesure révèle la valeur λ_1 (resp. λ_2 ou λ_3) valent :

$$p(\lambda = +\mu_0) = \left|\langle in|z+\rangle\right|^2 = |c_1|^2$$
$$p(\lambda = 0) = \left|\langle in|z0\rangle\right|^2 = |c_2|^2 \quad .$$
$$p(\lambda = -\mu_0) = \left|\langle in|z-\rangle\right|^2 = |c_3|^2$$

Le faisceau incident qui traverse l'analyseur est séparé aléatoirement en trois sous-faisceaux qui ne contiennent plus que des particules préparées dans un même état de spin selon Oz. A la sortie de l'analyseur, le nouveau vecteur d'état s'écrit respectivement :

$$|out\rangle = |z+\rangle \qquad \text{ou} \qquad |out\rangle = |z0\rangle \qquad \text{ou} \qquad |out\rangle = |z-\rangle .$$

On peut à nouveau éteindre deux sous-faisceaux pour n'en retenir qu'un seul dont on rectifie la trajectoire selon Oy. On est alors en mesure de prédire ce qu'on va observer si ce faisceau, disons, $|z+\rangle$, est analysé par un deuxième analyseur tourné d'un angle θ autour de l'axe Oy de propagation ou s'il est soumis à une induction constante.

1) Premier cas : action d'un deuxième analyseur de Stern-Gerlach. La grandeur mesurée n'est plus le moment magnétique selon Oz mais selon un axe faisant un angle θ avec Oz. L'opérateur correspondant s'écrit (cfr. annexe 1) :

$$M_\theta = R_{y,\theta}^{-1}\mu_B \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} R_{y,\theta} = \frac{1}{2}\mu_B \begin{pmatrix} \cos\theta & \frac{\sin\theta}{\sqrt{2}} & 0 \\ \frac{\sin\theta}{\sqrt{2}} & 0 & \frac{\sin\theta}{\sqrt{2}} \\ 0 & \frac{\sin\theta}{\sqrt{2}} & -\cos\theta \end{pmatrix}.$$

Les valeurs propres n'ont pas changé en sorte que la mesure fournit toujours une des réponses, $\lambda_1 = \mu_B$, $\lambda_2 = 0$ ou $\lambda_3 = -\mu_B$, mais les vecteurs propres ont changé :

$$|v_1\rangle = R_{y,\theta}^{-1}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos^2(\theta/2) \\ \frac{\sin\theta}{\sqrt{2}} \\ \sin^2(\theta/2) \end{pmatrix} \qquad |v_2\rangle = R_{y,\theta}^{-1}\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -\frac{\sin\theta}{\sqrt{2}} \\ \cos\theta \\ \frac{\sin\theta}{\sqrt{2}} \end{pmatrix} \qquad |v_3\rangle = R_{y,\theta}^{-1}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \sin^2(\theta/2) \\ -\frac{\sin\theta}{\sqrt{2}} \\ \cos^2(\theta/2) \end{pmatrix}$$

et les probabilités que la nouvelle mesure révèle les valeurs λ_i valent respectivement :

$$p(\lambda = +\mu_0) = \left|\langle z+|v_1\rangle\right|^2 = \cos^4(\theta/2)$$
$$p(\lambda = 0) = \left|\langle z+|v_2\rangle\right|^2 = \frac{\sin^2\theta}{2} \quad .$$
$$p(\lambda = -\mu_0) = \left|\langle z+|v_3\rangle\right|^2 = \sin^4(\theta/2)$$

Deuxième cas : action ultérieure d'une induction magnétique constante. Une induction appliquée à une particule de spin +1 sortant d'un premier dispositif de Stern-Gerlach a pour effet de le soumettre à un hamiltonien dont l'expression est connue :

$$H = -\vec{\mathbf{M}} \cdot \vec{B} = -\frac{\mu_B}{\sqrt{2}} \begin{pmatrix} \sqrt{2}B_z & B_x - iB_y & 0 \\ B_x + iB_y & 0 & B_x - iB_y \\ 0 & B_x + iB_y & \sqrt{2}B_z \end{pmatrix}.$$

Lorsque l'induction est orientée n'importe comment, la particule préparée dans l'état, $|z+\rangle = |0\rangle$, évolue selon une loi trop compliquée pour être détaillée. Deux cas particuliers suffisent à faire comprendre ce qui se passe soit lorsque l'induction est précisément alignée selon Oz ou selon un axe orthogonal, disons Ox. On trouve respectivement :

$$U|0\rangle = \exp[-\frac{i}{\hbar}Ht]|0\rangle = e^{i\mu_B B_z t}|0\rangle$$

$$U|0\rangle = \exp[-\frac{i}{\hbar}Ht]|0\rangle = \cos^2\frac{\mu_B B_x t}{2}|0\rangle + \frac{i}{\sqrt{2}}\sin(\mu_B B_x t)|1\rangle - \sin^2\frac{\mu_B B_x t}{2}|2\rangle.$$

On voit que dans le premier cas le vecteur d'état n'est que déphasé, ce qui n'entraîne aucune conséquence observable, tandis que dans le deuxième cas il rentre dans un état de superposition quantique variable au cours du temps.

Introduction à la théorie quantique de l'information.

Richard Feynman

Charles Bennett

Bits & Qubits.

L'information est une grandeur quantifiée et le quantum d'information est le bit ou le qubit selon la nature, classique ou quantique, du support physique qui l'abrite. L'un comme l'autre ne peuvent révéler, lors d'une mesure, que deux valeurs '0' ou '1'. Plus généralement, tout système possédant n états discrets peut encoder un alphabet à n symboles et le cas, n=2, correspond évidemment à l'encodage binaire. On trouve en annexe l'exemple de l'encodage d'un qutrit à l'aide d'une particule chargée de spin 1.

Tout système quantique binaire qui encode un qubit peut être décrit par un vecteur d'état qui occupe un espace de Hilbert à deux dimensions. Les états de base se notent : $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. L'orthonormation de cette base exige :

$\langle 0|0\rangle = \langle 1|1\rangle = 1$ et $\langle 0|1\rangle = \langle 1|0\rangle = 0$.

Bien que les contenus informationnels du bit et du qubit soient identiques, ce dernier présente sur son homologue classique un avantage déterminant pour la suite : non seulement il existe dans l'un ou l'autre de ses états de base mais encore, il peut exister sous la forme de n'importe quelle superposition linéaire de ces états de base,

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle = c_1\begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_2\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \qquad \left(|c_1|^2 + |c_2|^2 = 1\right).$$

Insistons sur le fait que l'existence des superpositions d'états quantiques ne signifie nullement que le contenu informationnel observable du qubit excède la valeur classique de 1 bit car toute lecture de son contenu passe par une mesure quantique qui a pour effet de projeter cet état sur un des états propres associés.

Il ne suffit pas d'être en mesure d'encoder un qubit encore faut-il pouvoir le manipuler. Plus précisément, il doit être possible de :

- filtrer le système choisi pour l'encodage du qubit dans chacun des états de base,
- préparer le système dans une superposition quelconque des états de base,
- maintenir le système dans son état de préparation, à l'abri d'interactions avec l'environnement,
- piloter à la demande tout changement d'état,
- prendre connaissance du contenu du qubit lors d'une mesure.

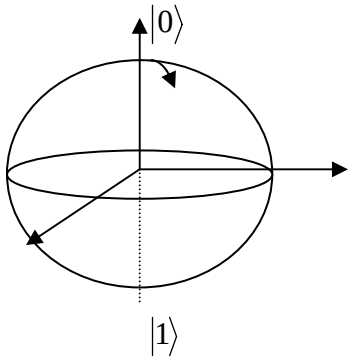
Nous commençons par montrer que ces opérations n'exigent que l'existence de deux manipulations, soit les transformations de Hadamard et de déphasage.

Préparation d'un qubit dans un état donné.

Lorsqu'une particule, par exemple un électron ou un photon, est émise par une source qui n'a fait l'objet d'aucune préparation préalable, elle se trouve dans un état de superposition indéterminé, $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$. Il est commode de réécrire cet état sous la forme trigonométrique,

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle \qquad (0 \le \theta \le \pi,\ \ 0 \le \varphi < 2\pi),$$

qui admet une représentation géométrique immédiate. Si les angles, θ et φ, définissent les coordonnées sphériques habituelles, ces états occupent les divers points de la sphère de Bloch. Les pôles N et S définissent les états de base, $|0\rangle$ et $|1\rangle$, tandis que l'équateur correspond aux états, $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right)$.



Pour préparer un faisceau de particules dans un état prédéfini, on procède en deux temps.

1) On commence par filtrer les particules qui émanent de la source dans l'un quelconque des états de base, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, par exemple. On y parvient habituellement en soumettant les particules à une mesure de l'observable dont les vecteurs propres définissent la base en question. Dans le cas de l'électron, c'est généralement la composante du spin selon Oz (dans le cas du photon, nous verrons que cela pourrait être sa polarisation rectiligne selon Ox). Un analyseur de Stern-Gerlach (resp. un cristal de calcite), suivi d'un écran absorbeur du sous-faisceau non désiré, fait l'affaire. On écrirait par exemple :

$$|\text{out}\rangle \underset{\text{renorm}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}|\text{in}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

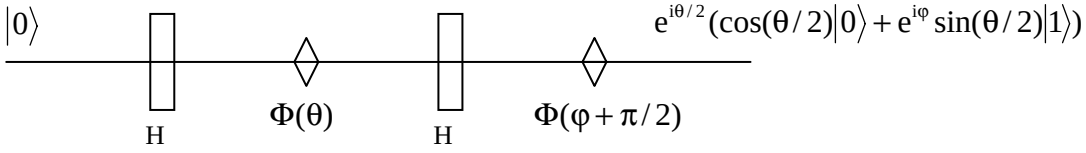
Il faut bien voir que cette transformation utilise un opérateur de projection non unitaire et qu'elle s'accompagne d'une perte d'information au niveau de l'écran absorbeur.

2) Une fois les particules filtrées dans l'état, $|0\rangle$, on peut les faire basculer dans l'état désiré, $\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$, en leur imposant, dans le bon ordre, quatre mesures supplémentaires n'utilisant que deux transformations, dites de Hadamard, H, et de déphasage, Φ. Sans préjuger de leur implémentation physique, nous commençons par en présenter les représentations matricielles. Elles s'écrivent traditionnellement :

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\Phi(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}.$$

Ces transformations sont unitaires. A ce titre, elles préservent la quantité d'information et elles agissent sur le vecteur d'état comme de véritables portes logiques quantiques. Sous réserve que l'implémentation physique de ces portes existe réellement, on construit l'état voulu en alignant quatre portes, deux de chaque sorte, dans l'ordre suivant :



On n'accorde aucune importance à la phase excédentaire $e^{i\theta/2}$: elle affecte globalement le vecteur d'état final et n'entraîne de ce fait aucune conséquence observable. La représentation matricielle de cet ensemble s'obtient tout naturellement en multipliant les matrices dans l'ordre inverse, ce qui donne :

$$\mathrm{U}(\theta,\varphi) = \Phi(\varphi+\pi/2)\cdot\mathrm{H}\cdot\Phi(\theta)\cdot\mathrm{H} = e^{i\theta/2}\begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ e^{i\varphi}\sin(\theta/2) & ie^{i\varphi}\cos(\theta/2) \end{pmatrix}$$

et on vérifie que l'on a bien :

$$\mathrm{U}(\theta,\varphi)|0\rangle = e^{i\theta/2}\begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ e^{i\varphi}\sin(\theta/2) & ie^{i\varphi}\cos(\theta/2) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = e^{i\theta/2}\begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix}$$
$$= e^{i\theta/2}(\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle)$$

On exprime le fait que fait que les portes H et Φ suffisent à construire l'état de superposition le plus général en disant qu'elles forment un couple universel pour la préparation du qubit isolé.

Transformation de l'état d'un qubit.

Les transformations de Hadamard et de déphasage résolvent du même coup le problème de la transformation d'état d'un qubit isolé. Le problème posé est le suivant : ayant préparé un qubit dans l'état initial connu,

$$|\text{in}\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle,$$

comment le faire basculer, éventuellement à une phase globale inessentielle près, dans l'état :

$$|\text{out}\rangle = \cos(\theta'/2)|0\rangle + e^{i\varphi'}\sin(\theta'/2)|1\rangle \ ?$$

La réponse est simple : il suffit de placer en série les quatre portes nécessaires pour passer de $|\text{in}\rangle$ à $|0\rangle$, puis les quatre portes requises pour repasser de $|0\rangle$ à $|\text{out}\rangle$. Au total, huit portes sont nécessaires qui, après simplifications, se réduisent à cinq :

$$\Phi(\varphi'+\pi/2)\cdot \text{H}\cdot\Phi(\theta'-\theta)\cdot \text{H}\cdot\Phi(-\varphi-\pi/2)|\text{in}\rangle = e^{i(\theta'-\theta)/2}|\text{out}\rangle.$$

Il reste à passer en revue quelques supports possibles de l'information quantique et à se convaincre que les portes de Hadamard et de déphasage existent effectivement dans chaque cas. Outre le cas de l'électron que nous rappelons brièvement et celui de la particule chargée de spin 1, reporté en annexe, nous considérons les états de polarisation du photon et ses états spatiaux.

Le qubit encodé grâce à une particule chargée de spin 1/2.

Ce premier cas est connu, il a servi d'illustration à l'énoncé des principes de la théorie quantique : rappelons que les deux états de moment magnétique de l'électron permettent l'encodage d'un qubit. Un appareil de Stern-Gerlach filtre un faisceau d'électrons en deux sous-faisceaux qui correspondent aux seuls états observables, $|0\rangle$ ou $|1\rangle$, et qui suivent des trajectoires différentes. On peut éteindre un des sous-faisceau, $|1\rangle$, par exemple et rectifier l'autre afin qu'il se réaligne sur la direction initiale sans modification de son filtrage $|0\rangle$. Les électrons restent filtrés aussi longtemps que le milieu extérieur n'exerce pas d'action directe sur eux.

Imaginons, à présent, que le faisceau filtré dans l'état $|0\rangle$ soit atténué au point qu'il ne contienne plus qu'un seul électron.

1) Porte de Hadamard.
Si on le fait passer dans un deuxième analyseur rectifié, en série avec le premier et qui fait un angle, θ, avec lui, il est facile de voir que ce deuxième analyseur agit comme une porte unitaire qui transforme le vecteur d'entrée, polarisé selon Oz, en un état de polarisation linéaire oblique :

$$|\text{out}\rangle = \hat{\text{P}}|\text{in}\rangle = \begin{pmatrix}\cos(\theta/2) & -\sin(\theta/2)\\ \sin(\theta/2) & \cos(\theta/2)\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{pmatrix} = \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle.$$

On voit que l'analyseur se comporte comme une porte logique dont la représentation matricielle coïncide avec la matrice inverse de rotation associée (cfr annexe 1) :

$$P(SG_\theta) = R^{-1}_{y,\theta} = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}.$$

Outre le cas trivial, $\theta = 0°$ qui restitue la matrice identité, on note le cas, $\theta = 90°$:

$$P(SG_{90°}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},$$

qui n'est pas exactement la matrice de Hadamard mais qui lui est, en fait, équivalente si on la combine avec une porte de déphasage, $\Phi(\pi)$. On a en effet :

$$H = P(SG_{90°})\Phi(\pi).$$

2) Porte de déphasage.
La porte de déphasage est associée au passage de l'électron qui sort du premier analyseur au travers d'une induction magnétique constante, pendant une durée qui dépend de la valeur du déphasage cherché. On sait que l'opérateur associé à cette manœuvre s'écrit :

$$P(B_z) = \begin{pmatrix} \exp[i\frac{\mu_B B_z}{2\hbar}t] & 0 \\ 0 & \exp[-i\frac{\mu_B B_z}{2\hbar}t] \end{pmatrix} = \exp[i\frac{\mu_B B_z}{2\hbar}t] \begin{pmatrix} 1 & 0 \\ 0 & \exp[-2i\frac{\mu_B B_z}{2\hbar}t] \end{pmatrix}$$

ce qui donne bien, toujours à une phase globale près, une transformation du type cherché :

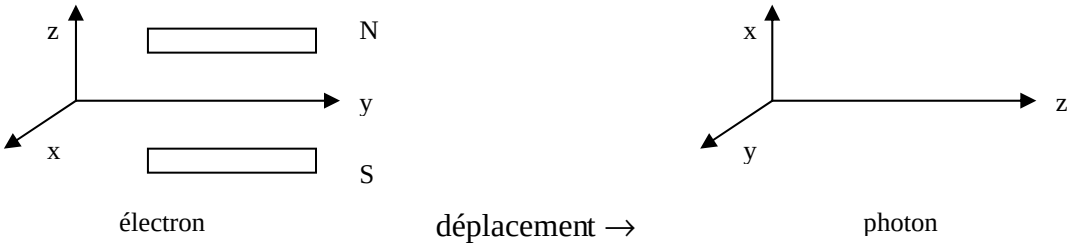
$$P(B_z) == \exp[i\frac{\mu_B B_z}{2\hbar}t]\Phi\left(-2\frac{\mu_B B_z}{2\hbar}t\right).$$

On trouvera, en annexe, comment encoder sur le même modèle un qutrit à l'aide d'une particule chargée de spin 1. Cela dit, il faut bien reconnaître que manipuler des qubits à l'aide de champs magnétiques est d'un inconfort total. Cette méthodologie permet certes de comprendre facilement les modes de raisonnement du traitement quantique de l'information mais elle est inapplicable concrètement. Il faut trouver autre chose.

Le qubit encodé grâce aux états de spin du photon.

Le photon possède un spin 1 en sorte qu'on s'attendrait à ce qu'il soit capable d'encoder un qutrit. Il n'en n'est rien car le photon ne possède que deux états observables de spin à savoir +1 et –1 (on n'observe jamais l'état 0). C'est une conséquence indirecte du fait que le photon est dépourvu de masse et que, de ce fait, il se déplace uniquement à la vitesse c.

Avant d'entrer dans les détails, il nous faut attirer l'attention sur un problème de notations. Un héritage historique fait qu'on a pris la fâcheuse habitude d'orienter différemment les axes pour le photon et l'électron. Le déplacement d'un électron dans un appareil de Stern-Gerlach se fait conventionnellement toujours selon Oy tandis qu'un photon progresse toujours selon Oz. On pourrait certes mettre un peu d'ordre à cela mais ce serait bousculer des traditions très ancrées dans la littérature.

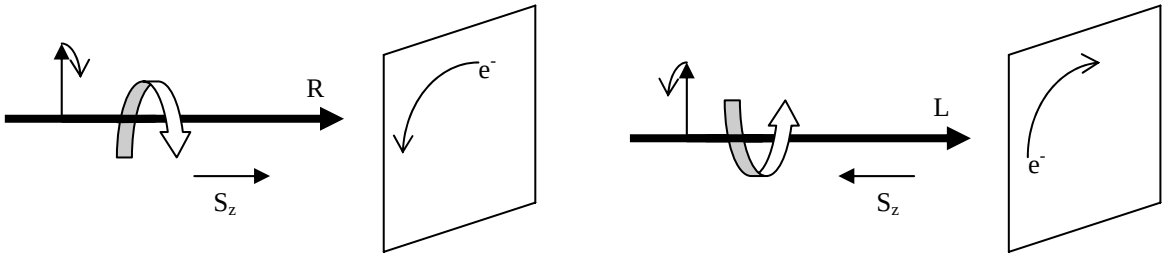


Que le photon soit un système à deux, et non trois, degrés de liberté interne est un fait expérimental bien établi qui découle de l'observation des états de polarisation de la lumière. On peut concilier cette observation avec un modèle théorique cohérent qui fait la connexion avec les deux états de spin autorisés mais cela nécessite d'entrer dans le détail de l'équation d'évolution du photon. Cette équation fait intervenir les variables externes continues de position et de quantité de mouvement et à ce titre son étude n'est pas strictement indispensable à l'élaboration d'une théorie quantique de l'information qui s'appuie sur l'existence d'états discrets. C'est pourquoi le lecteur intéressé par ce genre de détails se reportera à l'appendice intitulé « Equations d'onde ». On y montre que toutes les particules obéissent à une équation d'évolution qui incorpore les variables internes et externes, en particulier le spin. On y montre également que, dans le cas particulier du photon, ces équations coïncident, en fait, avec les équations de Maxwell et que, de fait, l'état de spin nul n'existe pas.

Par rapport à l'axe naturel que représente la direction de propagation, le photon possède deux états de moment angulaire associés chacun à une hélicité particulière. On distingue :

- le photon « vissé » à gauche, dont la composante, -1, du spin selon Oz est orientée en sens inverse de son mouvement
- le photon « vissé » à droite, dont la composante, +1, du spin selon Oz est orientée dans le sens de son mouvement

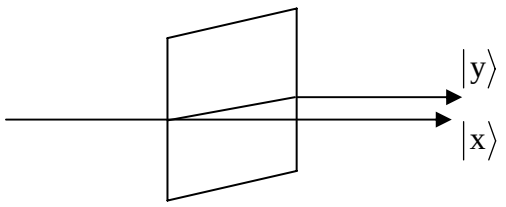
ou pour utiliser un langage consacré par l'usage, on distingue le photon polarisé circulairement à gauche (Left) de celui polarisé à droite (Right). On note habituellement ces deux états à l'aide des vecteurs de base, $|\mathrm{L}\rangle$ et $|\mathrm{R}\rangle$.



Comme souvent en physique des conventions ont été adoptées pour certaines grandeurs (le courant électrique, par exemple) à une époque où on ne connaissait pas l'agent atomique responsable. C'est également le cas pour la distinction entre polarisation circulaire gauche et droite. Les opticiens sont restés fidèles à la convention, héritée de la théorie électromagnétique de Maxwell, qu'une lumière est polarisée circulairement à droite (resp. à gauche) si un observateur qui la regarde venir vers lui doit un champ électrique qui tourne comme les aiguilles d'une montre (resp. en sens inverse). Par bonheur, un électron (négatif !) d'un milieu absorbant qui se trouverait sur le passage d'une lumière dont le champ électrique tournerait à droite entrerait en rotation contraire. Pour pouvoir justifier que cet électron acquiert un moment cinétique orienté dans le sens de progression de la lumière, il faut obligatoirement qu'il l'ait absorbé un photon vissé à droite.

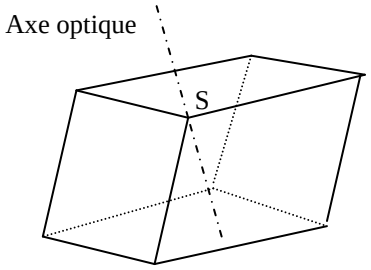
La base, $|L\rangle$ et $|R\rangle$, n'est pas la plus commode pour mettre en évidence expérimentalement les deux états du photon. La difficulté provient de ce que le photon n'étant pas chargé, il n'a pas de moment magnétique. Il est donc exclu de manipuler des photons à l'aide de champs magnétiques et finalement d'avoir directement accès à leur état de spin.

Fort heureusement, une propriété inattendue de la matière vole à notre secours. A condition d'être correctement taillés, certains cristaux, tels la calcite ou le quartz, ont la propriété de séparer les photons incidents en deux sous-faisceaux, dits ordinaire et extraordinaire, qui suivent des trajectoires généralement différentes et qui impriment aléatoirement deux points lumineux distincts mais fixes sur un écran placé en aval. Si l'on pose ce genre de cristal sur une feuille de papier où l'on a imprimé un point noir, on voit effectivement par transparence deux images grises. Si on fait tourner le cristal autour de l'axe de propagation, le point d'impact correspondant au rayon extraordinaire tourne autour de l'autre.



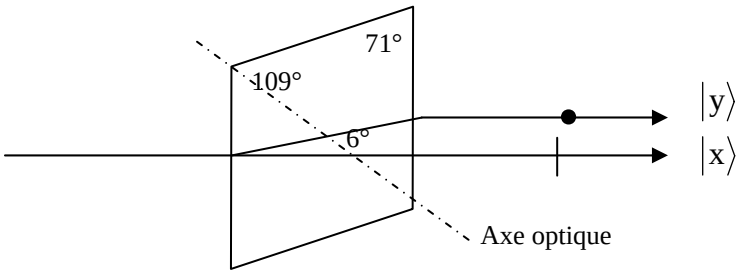
Notons respectivement, $|x\rangle$ et $|y\rangle$, les états des photons présents dans les deux sous-faisceaux. Pour l'instant, nous ignorons à quoi correspond cette différenciation. Il est tout à fait possible d'éteindre un des sous-faisceaux, disons, $|y\rangle$, en munissant le cristal d'un écran absorbeur du rayon extraordinaire, d'où il ne subsiste que le sous-faisceau filtré dans l'état, $|x\rangle$. On constate alors expérimentalement qu'un faisceau filtré de cette manière traverse intégralement un deuxième cristal équipé du même écran absorbeur s'il est orienté comme le premier mais qu'il est complètement arrêté s'il est tourné de 90° autour de la direction de propagation. On dit que chaque état, $|x\rangle$ ou $|y\rangle$, correspond à une polarisation linéaire distincte, l'une orientée selon un axe transversal, Ox, et l'autre selon un axe transversal orthogonal, Oy. C'est évidemment cette propriété d'orthogonalité qui permet aux états, $|x\rangle$ et $|y\rangle$, de former une base orthonormée. Il n'existe pas de photons polarisés longitudinalement et cela est en rapport avec le fait que le photon ne possède que deux états internes de spin.

Les directions Ox et Oy ne sont pas quelconques, elles sont imposées par les arrangements atomiques au sein de cristal. L'exemple typique est le cristal de calcite ($CaCO_3$). On peut se faire, comme suit, une idée de l'arrangement des atomes dans sa maille unité. On part d'un cube et on place un atome de calcium en chacun des huit sommets ainsi qu'au milieu de chacune des six faces. Ensuite, on place un atome de carbone au milieu de chacune des douze arêtes ainsi qu'au centre du cube. Chaque atome de carbone est immédiatement relié à trois oxygènes coplanaires qui présentent la particularité de dessiner des plans tous parallèles entre eux et perpendiculaires à une direction commune, baptisée axe optique, qui joint deux sommets diagonalement opposés. Il reste à déformer ce cube en forme de rhomboèdre pour obtenir une vue plus réaliste : chaque face est devenue un parallélogramme dont les angles valent, en alternance, invariablement 78° et 102°.



Les trois angles aboutissant à chaque sommet sont égaux mais leurs valeurs alternent de sommets en sommets voisins : par exemple, en S, ils valent tous environ 102° mais aux trois sommets voisins, ils valent environ 78°. L'axe optique passant par S fait le même angle (45.5°) avec les trois faces qui y aboutissent de même qu'avec les arêtes qui y aboutissent (63.8° cette fois). Il en résulte que l'axe optique est d'un axe de symétrie d'ordre trois.

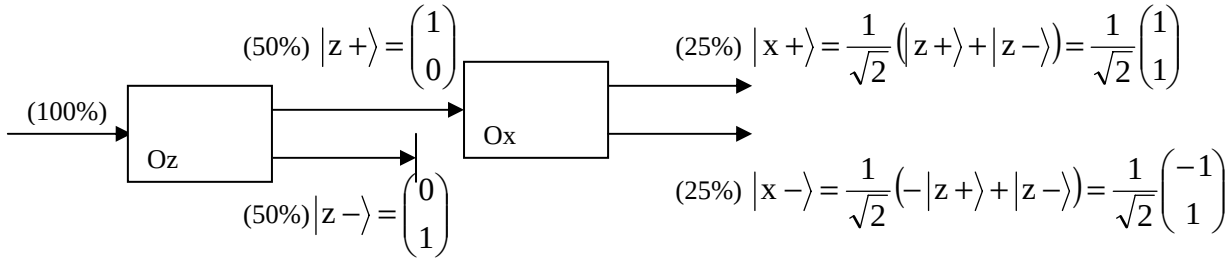
Voici plus précisément ce qu'on observe si on sélectionne un plan d'incidence passant par l'axe optique et perpendiculaire à l'une ou l'autre des trois faces aboutissant en S, définissant une des trois sections principales qui dessinent toutes un parallélogramme d'angles 109° et 71°.

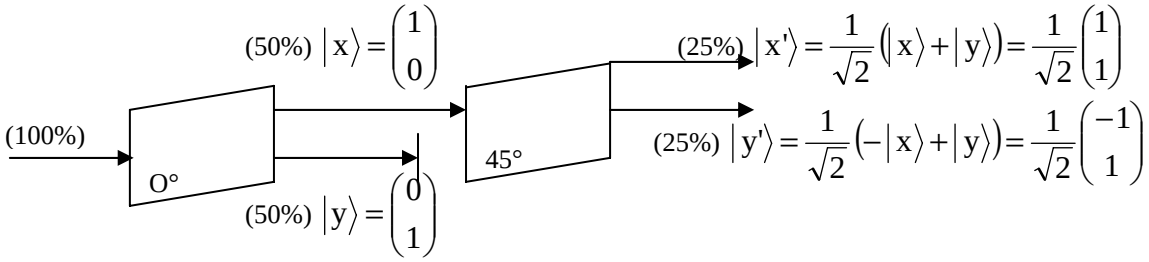


En conséquence de son anisotropie, le cristal de calcite présente deux indices de réfraction distincts, dits ordinaire, n_o, et extraordinaire, n_e. Il en résulte que le photon s'y déplace avec la vitesse, c/n_o, le long de l'axe optique, et c/n_e, dans n'importe quelle direction orthogonale à cet axe.

Tout photon incident, préparé initialement dans l'état de polarisation, $|x\rangle$, emprunte obligatoirement la trajectoire ordinaire qui respecte le la loi de la réfraction de Descartes alors que tout photon incident, préparé initialement dans l'état de polarisation, $|y\rangle$, emprunte obligatoirement la trajectoire extraordinaire qui ne respecte pas cette loi. Si le photon incident n'a fait l'objet d'aucune préparation particulière, il se trouve dans un état de superposition équitable, $c_1|x\rangle + c_2|y\rangle$ $(|c_1|^2 = |c_2|^2 = 1/2)$, et tout se passe comme s'il empruntait simultanément les deux trajectoires.

La calcite agit donc sur un faisceau de photons comme un appareil de Stern-Gerlach le fait sur un faisceau d'électrons : il sépare aléatoirement les particules en deux sous faisceaux de polarisations différentes tout en leur imprimant des trajectoires distinctes. On peut illustrer cette analogie par l'exemple simple suivant :





La première figure concerne l'électron et la seconde le photon. Dans les deux cas, le premier analyseur est caractérisé respectivement par l'opérateur, σ_z (resp. P_x) = $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$, d'états propres, $\begin{pmatrix}1\\0\end{pmatrix}$ et $\begin{pmatrix}0\\1\end{pmatrix}$, qui servent d'états de base. Le deuxième analyseur est caractérisé par l'opérateur, σ_x (resp. $P_{45°}$) = $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ d'états propres, $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ et $\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix}$, dans la même base. On reconnaît au passage deux des matrices de Pauli. La troisième interviendrait si on mesurait la composante du spin selon la direction de propagation. Les observables correspondants seraient les opérateurs, σ_y (resp. P_c) = $\begin{pmatrix}0 & -i\\i & 0\end{pmatrix}$, d'états propres, $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$ et $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$.

Dans le cas du photon, cet opérateur est tout naturellement associé à la mesure de son hélicité dans la base mentionnée et les états propres sont les deux états de polarisation circulaires, $|R\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}$ et $|L\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix}$.

On passe donc des états de polarisation circulaire aux états de polarisation linéaire par les formules de changement de base :

$$\begin{aligned}|R\rangle &= \frac{1}{\sqrt{2}}\left(|x\rangle + i|y\rangle\right)\\ |L\rangle &= \frac{1}{\sqrt{2}}\left(|x\rangle - i|y\rangle\right)\end{aligned} \quad \Leftrightarrow \quad \begin{aligned}|x\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle + |L\rangle\right)\\ |y\rangle &= \frac{1}{i\sqrt{2}}\left(|R\rangle - |L\rangle\right)\end{aligned},$$

soit, en abrégé,

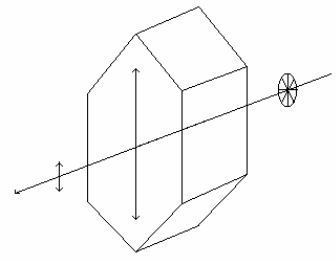
$$\begin{pmatrix}|R\rangle\\ |L\rangle\end{pmatrix} = T^{-1}\begin{pmatrix}|x\rangle\\ |y\rangle\end{pmatrix} \quad \Leftrightarrow \quad \begin{pmatrix}|x\rangle\\ |y\rangle\end{pmatrix} = T\begin{pmatrix}|R\rangle\\ |L\rangle\end{pmatrix},$$

où on a posé :

$$T = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -i & i\end{pmatrix} \quad \Leftrightarrow \quad T^{-1} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}.$$

Le modèle exposé suppose l'utilisation d'analyseurs en calcite ou en quartz. D'autres analyseurs existent, tels la tourmaline, qui polarisent la lumière grâce à un pouvoir d'absorption très contrasté entre une direction transversale principale, Ox, et son orthogonale, Oy (dichroïsme). Si l'épaisseur traversée est suffisante, le faisceau sortant est pratiquement pur, avec tous les photons dans l'état, $|x\rangle$. C'est évidemment l'arrangement spécifique des atomes dans le cristal qui privilégie une direction transversale par rapport à son orthogonale.

L'exemple de la tourmaline est relativement académique car, en pratique, le contraste modéré entre les coefficients d'absorption nécessite de gros cristaux difficiles à réaliser. De plus l'absorption parallèlement à l'axe optique est loin d'être négligeable et enfin, elle varie avec la longueur d'onde. La version moderne du polaroïd est produite par étirement de longues chaînes hydrocarbonées d'une feuille d'alcool polyvinyllique.



Bien que capable de polariser linéairement la lumière dans une direction transversale quelconque, le polaroïd possède des inconvénients irrémédiables pour les tâches que nous avons en vue. Par exemple, s'il prépare sans problème un flux de photons dans un même état de polarisation rectiligne, il est incapable de manipuler ces photons sans absorption. En particulier, le fait de travailler par absorption le rend incapable de simuler une porte logique unitaire, de Hadamard par exemple. En effet, pour faire basculer la polarisation rectiligne des photons d'un angle θ, on interpose un deuxième polaroïd tourné de cet angle par rapport au premier. Il est exact que les photons sortants auront la polarisation désirée mais c'est au prix de la disparition de $\sin^2\theta$ photons, en moyenne, absorbés par le polaroid. En d'autres termes, tout dispositif de polarisation par dichroïsme est partiellement destructeur de photons et donc représente une perte inadmissible d'information.

Porte logiques qui agissent sur les états de polarisation du photon.

La séparation des sous-faisceaux opérée par l'analyseur de calcite est commode pour filtrer des photons dans un état de base mais elle est une nuisance pour toutes les opérations logiques ultérieures pour lesquelles on veut pouvoir profiter des possibilités de superpositions quantiques. Une remarque similaire a déjà été faite pour l'analyseur de Stern-Gerlach et on a vu qu'il fallait rectifier les trajectoires des électrons à sa sortie le long de l'axe de propagation. Par bonheur cette rectification est beaucoup plus facile à réaliser avec des photons : il suffit de tailler la lame de calcite perpendiculairement à l'axe optique et de l'éclairer en incidence normale. Dans ce cas, les trajectoires des photons à la sortie demeurent confondues.

1) Porte de Hadamard.

Atténuons la source au point qu'elle n'émette qu'un seul photon à la fois et filtrons ce photon dans l'état, $|0\rangle = |x\rangle$. Faisons-le passer dans un deuxième analyseur, en série avec le premier et qui fait un angle, θ, avec lui. Il nous faut connaître l'opérateur associé à la mesure de la polarisation linéaire selon le nouvel axe Ox*. Ici se présente une difficulté du fait que les matrices de rotation applicables aux particules de spin 1 n'ont été écrites (en annexe) que pour les états propres selon l'axe de propagation, soit pour les états $|R\rangle$ et $|L\rangle$. Notant avec une étoile les états exprimés dans la base qui est tournée de, -θ, on a trouvé (cfr. annexe) :

$$\begin{pmatrix} |R^*\rangle \\ |L^*\rangle \end{pmatrix} = R^{-1}_{z,\theta} \begin{pmatrix} |R\rangle \\ |L\rangle \end{pmatrix} = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} |R\rangle \\ |L\rangle \end{pmatrix}$$

Heureusement nous connaissons les transformations qui font passer de la base, $|x\rangle$ et $|y\rangle$, à la base, $|R\rangle$ et $|L\rangle$:

$$\begin{pmatrix} |x\rangle \\ |y\rangle \end{pmatrix} = T \begin{pmatrix} |R\rangle \\ |L\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} |R\rangle \\ |L\rangle \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} |x^*\rangle \\ |y^*\rangle \end{pmatrix} = T \begin{pmatrix} |R^*\rangle \\ |L^*\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} |R^*\rangle \\ |L^*\rangle \end{pmatrix},$$

d'où on tire la relation cherchée :

$$\begin{pmatrix} |x^*\rangle \\ |y^*\rangle \end{pmatrix} = TR_{z,\theta}T^{-1}\begin{pmatrix} |x\rangle \\ |y\rangle \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} |x\rangle \\ |y\rangle \end{pmatrix}.$$

$\Re = TR_{z,\theta}T^{-1}$ est la matrice de rotation qui agit sur le vecteur d'état dans la base ($|x\rangle$ et $|y\rangle$). L'opérateur associé à la mesure effectuée par un polariseur orienté sous l'angle θ par rapport à Ox s'écrit finalement :

$$Pol_\theta = \Re^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\Re = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}$$

soit la même matrice que pour un analyseur de Stern-Gerlach dans le cas du spin 1/2, sauf que l'angle est doublé. Les vecteurs propres de Pol_θ se notent :

$$|v_1\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \Re^{-1}|0\rangle \qquad |v_1\rangle = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} = \Re^{-1}|1\rangle,$$

en sorte que ce polariseur incliné sous l'angle, θ, agit comme une porte logique :

$$P_\theta = \Re^{-1} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

On note que pour θ=45°, on retrouve la porte, $P(SG_{90°})$ apparentée à la porte de Hadamard.

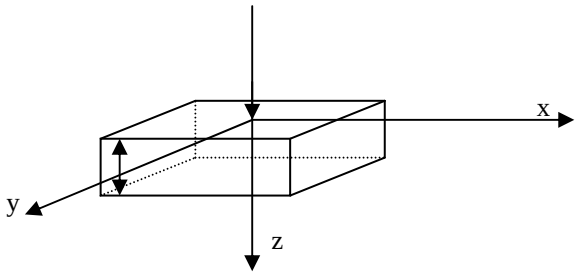
2) Porte de déphasage.

Une lame isotrope, à faces parallèles, d'indice, n, et d'épaisseur, d, orientée perpendiculairement au trajet d'un photon individuel ne fait que le ralentir temporairement. Son vecteur d'état s'en trouve globalement multiplié par un facteur de phase, $e^{i\varphi}$ $\left(\varphi = \frac{2\pi nd}{\lambda}\right)$, qu'aucune mesure ne peut révéler :

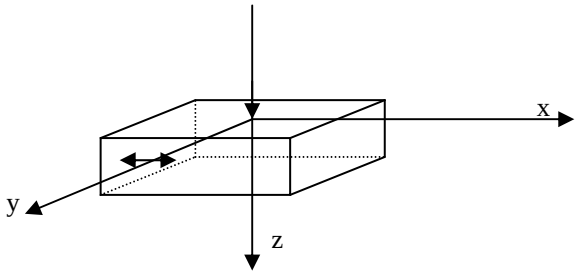
$$|\psi_{in}\rangle = c_1|x\rangle + c_2|y\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \qquad \Rightarrow \qquad |\psi_{out}\rangle = e^{i\varphi}|\psi_{in}\rangle \qquad \left(\varphi = \frac{2\pi}{\lambda}nd\right).$$

La situation ne diffère pas fondamentalement si on taille la lame de calcite, d'épaisseur, d, parallèlement à l'axe optique et qu'on l'éclaire en incidence normale. Dans ce cas particulier, les trajectoires ordinaire et extraordinaire demeurent confondues avec la direction incidente et les photons « voient » tous le même indice de réfraction, n_o, d'où ils subissent à nouveau le même ralentissement. Cette lame se comporte comme le ferait n'importe quelle lame isotrope.

.



2ème cas : voyons à présent ce qui se passe si on taille la lame de calcite perpendiculairement à l'axe optique et qu'on l'éclaire encore en incidence normale.



Les trajectoires ordinaire et extraordinaire demeurent confondues avec la direction incidente mais à présent, les photons « voient » deux indices de réfraction distincts, n_o et n_e, ($n_o > n_e$) selon leur état de polarisation. Un photon préparé initialement dans un état $|x\rangle$ (resp. $|y\rangle$) subirait un déphasage $\varphi_o = \frac{2\pi}{\lambda} n_o d$ (resp. $\varphi_e = \frac{2\pi}{\lambda} n_e d$). Un photon incident n'ayant subi aucune préparation particulière est nécessairement dans un état de superposition quantique, $|\psi_{in}\rangle = c_1|x\rangle + c_2|y\rangle$ et dans ce cas, un déphasage mutuel supplémentaire prend naissance capable de transformer une polarisation linéaire (si c_1 et c_2 sont réels) en polarisation elliptique. La seule exception interviendrait si par hasard le déphasage valait 0 ou π, auquel cas la polarisation resterait linéaire mais dans une direction modifiée. On écrit dans le cas général :

$$|\psi_{in}\rangle = c_1|x\rangle + c_2|y\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \qquad \Rightarrow \qquad |\psi_{out}\rangle = c_1 e^{i\varphi_o}|x\rangle + c_2 e^{i\varphi_1}|y\rangle .$$

Dans la représentation matricielle habituelle des vecteurs de base, $|x\rangle$ et $|y\rangle$, l'opérateur unitaire qui est associé à cette manœuvre se note simplement :

$$P_{lame\perp} = \begin{pmatrix} e^{i\varphi_o} & 0 \\ 0 & e^{i\varphi_e} \end{pmatrix} = e^{i\varphi_o} \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\varphi_e - \varphi_o)} \end{pmatrix}.$$

On peut interpréter ces résultats en disant que cette lame introduit un phase globale inessentielle plus un déphasage relatif, valant :

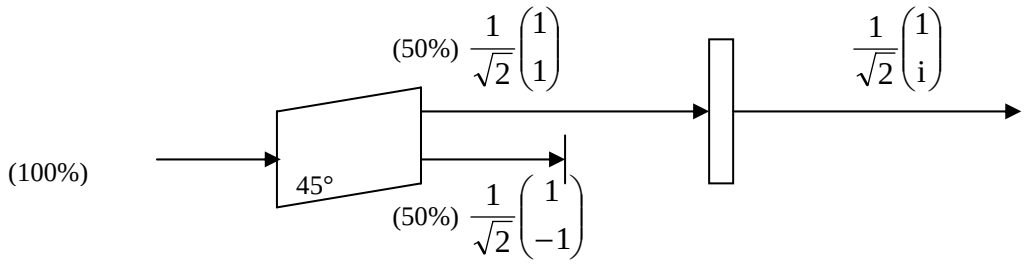
$$\Delta\varphi = \varphi_e - \varphi_o = \frac{2\pi}{\lambda}(n_e - n_o)d .$$

On note que l'épaisseur minimum, d, d'une telle lame qui garantit un déphasage donné varie comme l'inverse de la différence, n_e-n_o. La difficulté qu'il peut y avoir à tailler une lame fine fait que l'on peut avoir intérêt à choisir un matériau pour lequel cette différence n'est pas trop importante. Ce n'est pas vraiment le cas de la calcite à laquelle il n'est pas rare qu'on préfère le mica. Cela étant dit nous ignorerons désormais ces contingences inessentielles. Les lames suivantes sont couramment utilisées :

- Si $\Delta\varphi$ vaut 2π, la lame est dite « onde » et la polarisation du photon n'est pas modifiée à la sortie de la lame.
- Si $\Delta\varphi$ vaut π, la lame est dite « demi-onde » et la polarisation du photon est modifiée comme suit : si elle était linéaire, elle le reste en basculant simplement dans les quadrants de parité contraire et si elle était circulaire, elle s'inverse de gauche à droite et inversement (le photon change d'hélicité).
- Si $\Delta\varphi$ vaut $\pi/2$ (resp. $3\pi/2$), la lame est dite « quart d'onde » et la polarisation du photon est modifiée comme suit : si la polarisation était linéaire, inclinée à 0° ou 90° par rapport à l'axe de la lame, elle permute ces deux possibilités, si la polarisation linéaire était inclinée à 45°, elle devient circulaire droite (resp. gauche). Pour tout autre angle la polarisation devient elliptique.

Il existe d'autres dispositifs, tels les rhomboïdes de Fresnel ou de Mooney qui sont capables de produire un déphasage relatif entre les polarisations x et y. Ils sont basés sur le principe de la différence de déphasages lors d'une réflexion totale. Ainsi un verre d'indice 1.51 induit un déphasage de 45° lors d'une réflexion totale sous un angle de 54.6°. Deux réflexions totales induisent donc un déphasage de 90°. L'avantage de tels dispositifs est qu'ils sont effectifs quelle que soit la fréquence de la lumière. Des variantes existent utilisant des matériaux biréfringents à pouvoir optique que nous ne détaillons pas ici.

On se convaincra que le dispositif suivant qui aligne en série un polariseur linéaire incliné à 45° et une lame quart d'onde réalise la préparation d'un photon polarisé circulairement.



Insistons sur le fait que dans ce montage, l'existence d'un écran absorbeur au niveau du polariseur empêche celui-ci d'agir comme une porte logique de représentation matricielle,

$$\mathrm{Pol}_{45^\circ} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.$$

Il agit plutôt comme un projecteur non unitaire de représentation,

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}.$$

On vérifie que le vecteur d'état s'écrit à sa sortie :

$$\left|\text{out}\right\rangle \underset{\text{renorm}}{=}\frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}\begin{pmatrix}c_1\\c_2\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}.$$

Par contre la lame quart d'onde est une porte logique de représentation,

$$P_{\text{lame}\perp}=\begin{pmatrix}1 & 0\\0 & e^{i\pi/2}\end{pmatrix}=\begin{pmatrix}1 & 0\\0 & i\end{pmatrix}.$$

Résumé comparatif des qubits encodés sur base des états internes de l'électron et du photon.

Ces deux encodages sont nettement ressemblants et le polariseur linéaire joue un rôle analogue à l'analyseur de Stern-Gerlach. On a le tableau suivant :

Observable, $\hat{O}$	$S_{z,\theta}=\frac{1}{2}\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}$	$\text{Pol}_{x,\theta}=\begin{pmatrix}\cos 2\theta & \sin 2\theta\\ \sin 2\theta & -\cos 2\theta\end{pmatrix}$
Vecteurs propres de $\hat{O}$	$\begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix}=R^{-1}\left\|0\right\rangle$ $\begin{pmatrix}-\sin\frac{\theta}{2}\\ \cos\frac{\theta}{2}\end{pmatrix}=R^{-1}\left\|1\right\rangle$	$\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}=R^{-1}\left\|0\right\rangle$ $\begin{pmatrix}-\sin\theta\\ \cos\theta\end{pmatrix}=R^{-1}\left\|1\right\rangle$
Matrice de rotation, R	$R=\begin{pmatrix}\cos\frac{\theta}{2} & \sin\frac{\theta}{2}\\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}$	$R=\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$
Porte logique, P	$R=\begin{pmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}$	$\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$

Dans les deux cas, la porte logique, P, mène directement à la porte de Hadamard et la porte de déphasage s'obtient en contraignant la particule à traverser une épaisseur bien choisie de champ magnétique dans le cas de l'électron et de cristal anisotrope dans le cas du photon.

Il ne faudrait toutefois pas conclure que l'analogie est totale entre les traitements de l'information de l'électron et du photon. Ce serait perdre de vue que le photon, au contraire de l'électron, possède le spin 1. Cela se traduit par un doublement de l'angle dans le cas du photon et à une réaction différente des vecteurs d'état lors d'une rotation des axes de référence.

Les lois de Malus.

Les états de polarisation de la lumière sont enseignés classiquement depuis longtemps dans le cadre de la théorie de Maxwell. Les prédictions théoriques respectent la réalité expérimentale mais le modèle quantique va plus loin en affirmant que la notion de polarisation conserve un sens lorsqu'on considère un photon isolé. Il est amusant de réaliser aujourd'hui que les expériences effectuées par Malus dès 1807 constituent, en fait, un chapitre à part entière de la mécanique quantique.

1ère loi. Envoyons un photon polarisé circulairement vers un polariseur dont la direction principale est orientée selon Ox ($\theta = 0$). Son vecteur d'état s'écrit initialement :

$$|\text{in}\rangle = \frac{1}{\sqrt{2}}(|\text{x}\rangle + \text{i}|\text{y}\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ \text{i}\end{pmatrix}.$$

A la sortie du polariseur, le vecteur d'état vaudra :

$$|\text{out}\rangle = |\text{x}\rangle \qquad \text{ou} \qquad |\text{out}\rangle = |\text{y}\rangle .$$

Cela se produira aléatoirement avec les probabilités suivantes :

$$p_x = \left|\langle \text{in}|\hat{P}_x\right|^2 = \left|\frac{1}{\sqrt{2}}(1 \;\; \text{i})\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\right|^2 = \frac{1}{2}$$
$$p_y = \left|\langle \text{in}|\hat{P}_y\right|^2 = \left|\frac{1}{\sqrt{2}}(1 \;\; \text{i})\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right|^2 = \frac{1}{2}$$

2ème loi. Considérons, à présent, un photon qui a été préparé dans l'état, $|\text{x}\rangle = \begin{pmatrix}1\\ 0\end{pmatrix}$, du fait de son passage dans un premier polariseur et faisons lui traverser un analyseur faisant l'angle θ avec le premier. La probabilité pour qu'il en sorte dans l'état, $|\text{x}\rangle$, vaut :

$$p_x = \left|\langle \text{in}|\hat{P}_\theta\right|^2 = \left|\frac{1}{\sqrt{2}}(1 \;\; 0)\begin{pmatrix}\cos^2\theta & \sin\theta\cos\theta\\ \sin\theta\cos\theta & \sin^2\theta\end{pmatrix}\right|^2 = \cos^2\theta$$

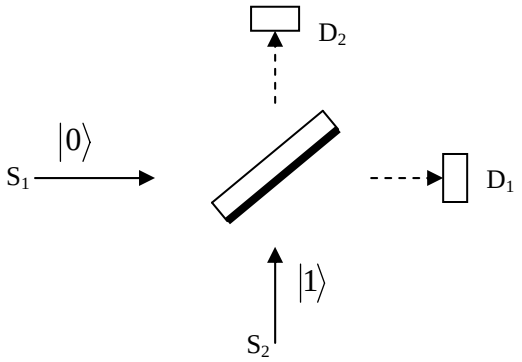
et la probabilité pour qu'il en sorte dans l'état, $|\text{y}\rangle$, vaut, $\sin^2\theta$. Ce sont bien les lois de Malus.

L'encodage du qubit sur base des états spatiaux du photon.

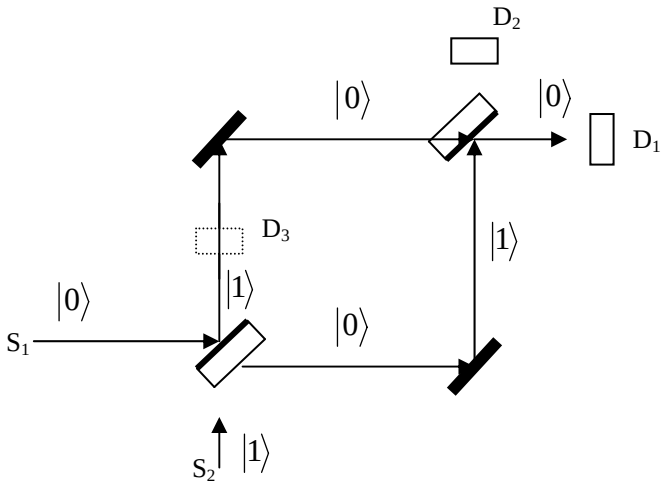
Le photon autorise au moins une autre méthode d'encodage du qubit, basée non plus sur ses états internes de spin mais sur ses états externes de trajectoire. Imaginons un photon se déplaçant initialement horizontalement (ou verticalement) et qui traverse une lame semi-

transparente orientée à 45°. C'est une lame dont une face est recouverte d'une couche mince diélectrique réfléchissante. Dans la discussion qui suit, on ne tient pas compte des réflexions multiples que l'on éradique par une technologie appropriée.

A la sortie de la lame, les seules trajectoires autorisées sont horizontale et verticale. Ignorant les états internes de spin, on peut donc encoder, en permanence, les deux états possibles du photon par les vecteurs d'état, $|h\rangle = |0\rangle$ et $|v\rangle = |1\rangle$. Deux détecteurs, D_1 et D_2, sont placés en aval de telle manière que D_1 ne détecte que les photons qui sortent de la lame dans l'état, $|h\rangle = |0\rangle$, et D_2 ne détecte que ceux qui sortent dans l'état, $|v\rangle = |1\rangle$. Lorsqu'on monte cette expérience, on constate que la détection d'un photon suit une loi totalement probabiliste : il est impossible de prédire en toute certitude quel détecteur enregistrera l'arrivée d'un photon unique qui traverse une lame semi-transparente. Certes, chacun a une chance sur deux d'enregistrer l'arrivée d'un photon individuel mais lorsque l'expérience est recommencée un grand nombre de fois, la succession des détections forme une suite, $\{D_1,D_1,D_2,D_1,\ldots\}$ totalement aléatoire au sens que la théorie de l'information prête à ce terme, soit présentant une entropie algorithmique de 1bit/symbole.



Ce n'est donc qu'au moment de la détection que l'on sait quelle trajectoire le photon a suivi dans la lame. Tant que cette détection n'est pas faite, il y a lieu de considère que le photon emprunte potentiellement les deux trajectoires dans un état de superposition, $c_1|h\rangle + c_2|v\rangle$. Une lame semi-transparente ne favorise aucune des deux émergences possibles d'où il résulte que les coefficients c_1 et c_2 sont de modules égaux à $1/\sqrt{2}$. Toutefois cela laisse planer une indétermination sur leur phase ou plus précisément sur leur différence de phase.



On lève l'indétermination en réalisant l'expérience suivante dont le résultat heurte l'intuition. On complète le montage précédent en ajoutant deux miroirs parfaitement réfléchissants et une deuxième lame semi réfléchissante. Enfin, on déplace les détecteurs comme indiqué sur la figure : l'ensemble constitue un interféromètre de Mach-Zender.

Une observation surprenante intervient à ce stade : à condition de garantir l'égalité des longueurs des deux bras de l'interféromètre, on constate que même en recommençant l'expérience un grand nombre de fois, seul le détecteur D_1 (resp. D_2) enregistre l'arrivée d'un photon émis en S_1 (resp. en S_2). On réalise qu'une interprétation classique consistant à imaginer que chaque fois qu'un photon rencontre une lame semi-transparente, il choisit au hasard une des deux trajectoires possibles, ne tient pas la route. Si elle était correcte, les deux détecteurs cliqueraient en moyenne une fois sur deux.

Le fait est que le photon emprunte virtuellement les deux trajectoires et qu'un phénomène d'interférence quantique prend naissance entre ces deux éventualités. Le formalisme quantique permet d'en rendre compte en détaillant les superpositions d'états du photon. Considérons un photon émis par la source S_1 (resp. S_2), il est dans l'état, $|0\rangle$, (resp. $|1\rangle$). Quelle que soit la trajectoire individuelle considérée, il rencontre un miroir parfait orienté à 45° et une lame semi-transparente. L'opérateur, nécessairement unitaire, associé au miroir possède la représentation matricielle suivante :

$$\mathrm{M} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On vérifie qu'il transforme effectivement l'état, $|\mathrm{h}\rangle = |0\rangle$, en l'état, $|\mathrm{v}\rangle = |1\rangle$, et réciproquement. L'opérateur associé à la lame semi-transparente possède une représentation qui dépend de la position de la face diélectrique par rapport à l'incidence en provenance de S_1 : on distingue les deux cas,

$$\mathrm{L}_{\text{gauche}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad \mathrm{L}_{\text{droite}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Par exemple, un photon émis en S_1 (resp. S_2) sort de la première lame dans la superposition d'état, $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, (resp. $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$). Que le photon soit émis en S_1 ou en S_2, il rencontre successivement et dans cet ordre une lame gauche, un miroir puis une lame droite. La représentation matricielle de l'opérateur globalement associé à l'interféromètre s'obtient en multipliant de droite à gauche les matrices associées à chacun :

$$\mathrm{U}_{\mathrm{M-Z}} = \mathrm{L}_{\text{droite}}\mathrm{M}\mathrm{L}_{\text{gauche}} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Il se peut qu'on trouve d'autres expressions dans la littérature qui dépendent de l'orientation de la couche diélectrique des lames semi-transparentes mais elles sont équivalentes. Quoi qu'il en soit, on voit qu'un photon émis en S_1, qui se trouve donc initialement dans l'état,

$|h\rangle = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, se trouvera dans l'état, $\begin{pmatrix}-1\\0\end{pmatrix} = -|0\rangle$, à la sortie de l'interféromètre. Sa détection se fera obligatoirement en D_1 ce que l'expérience confirme. On raisonnerait de même pour S_2 et D_2.

On précise que cette analyse ne permet en aucune manière de dire quel bras de l'interféromètre le photon a suivi avant d'être détecté. Les principes de la mécanique quantique affirment d'ailleurs que cette question est vide de sens. Elle ne prendrait de sens que si on plaçait un troisième détecteur en D_3, par exemple. Si on fait cela, on observe que celui-ci clique en moyenne une fois sur deux tandis que D_1 et D_2 cliquent en moyenne une fois sur quatre ! Que s'est-il passé pour que le phénomène d'interférence disparaisse ? Ce détecteur agit comme un appareil de mesure qui détruit la superposition due à la première lame. Soit D_3 a réellement détecté le photon et il est absorbé dans l'état $|1\rangle$, soit il n'a rien détecté et le photon s'en trouve projeté dans l'état, $|0\rangle$. C'est dans cet état, $|0\rangle$, qu'il va aborder la deuxième lame avec des probabilités égales d'être détecté en D_1 ou en D_2.

1) Porte de Hadamard.
La lame semi-transparente mène directement à la porte de Hadamard. On peut régler l'épaisseur de la lame pour que le photon transmis ne subisse aucun déphasage observable (ou si on préfère un déphasage multiple de 2π) mais on ne peut éviter le déphasage de π dû à la réflexion du photon incident sur un milieu plus réfringent. On constate qu'un photon émanant de S_1 (resp. S_2), donc dans l'état $|0\rangle$ (resp. $|1\rangle$), ressort de la lame dans la superposition d'état, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (resp. $\frac{1}{\sqrt{2}}(e^{i\pi}|0\rangle + |1\rangle)$). Au bilan la porte se note indifféremment par sa table logique :

$$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix} \quad \rightarrow \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$
$$|1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix} \quad \rightarrow \quad \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix}$$

ou par la représentation matricielle de la transformation unitaire, L_{gauche} ou L_{droite}, qu'elle représente selon l'orientation de la face diélectrique :

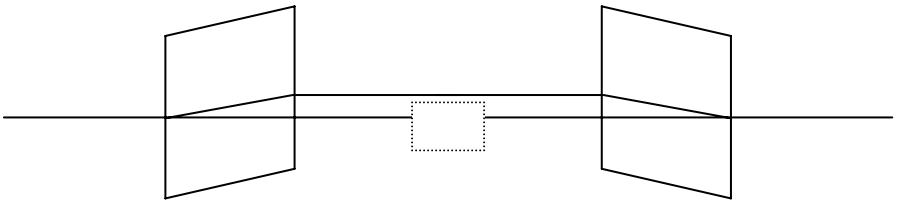
$$L_{gauche} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\-1 & 1\end{pmatrix} \qquad L_{droite} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\1 & 1\end{pmatrix}.$$

2) Porte de déphasage.
L'insertion d'une lame retardatrice isotrope sur un des bras de l'interféromètre provoque un déphasage sélectif dont la valeur se règle, comme d'habitude, en fonction de l'épaisseur, d, et de l'indice, n, de la lame : $\Delta\varphi = \frac{2\pi}{\lambda} nd$.

Le principe de l'interféromètre.

L'encodage du qubit à l'aide d'une lame semi-transparente est certes un peu encombrant mais il présente l'avantage de séparer nettement les trajectoires des états individuels. Cela permet de manipuler plus facilement chaque trajectoire individuellement. Dans un appareil de Stern-Gerlach ou dans un cristal de calcite cette séparation est également présente mais elle est plutôt une gêne car les opérateurs associés aux analyseurs ne sont simples que si les trajectoires des particules sont rectifiées selon la direction initiale.

Cela dit deux cristaux de calcite mis en tête-bêche constituent également un interféromètre et on pourrait imaginer manipuler l'information rien qu'en altérant la phase du photon sur l'un ou l'autre trajet.



Sources non polarisées, états impurs impossibles à cloner.

Considérons une source d'électrons ou de photons il importe peu. On suppose que cette source est quelconque au point de ne privilégier aucun état dans quelqu'espace de Hilbert que ce soit : une telle source est dite non polarisée. On entend par là qu'un analyseur, peu importe l'observable qu'il représente, partage le faisceau émis en deux sous faisceaux d'égales intensités. C'est effectivement ce qu'on observe expérimentalement dans un grand nombre de cas.

Imaginons que l'on atténue la source au point qu'elle n'émette les particules qu'au compte-gouttes. La question est vide de sens de se demander à quoi ressemble le vecteur d'état de chaque individu émis par la source. En particulier, il n'existe aucune procédure expérimentale capable de révéler des coefficients, c_1 et c_2, dans l'écriture de son état, que l'on espérerait sous la forme,

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle .$$

C'est une conséquence immédiate de la théorie de la mesure quantique qu'il s'agit typiquement d'un faux problème car toute tentative de lecture passerait par une mesure quantique qui détruirait l'état observé pour le remplacer par sa projection sur l'espace propre associé au résultat de cette mesure.

Pourtant, en admettant que le comportement de la source soit stable dans le temps, un observateur pourrait tenter de contourner l'obstacle en procédant de la manière suivante. En analysant chaque électron un à un, il devrait lui être possible d'observer quel canal ils empruntent au travers d'un analyseur de Stern-Gerlach orienté selon Oz. Lorsqu'un grand

nombre, N, d'électrons auront été analysés soit N_+ dans l'état, $|z+\rangle$, et N_- dans l'état, $|z-\rangle$, les rapports N_{z+}/N et N_{z-}/N se rapprocheront d'autant plus de $|c_1|^2$ et de $|c_2|^2$ que N sera grand. Si l'on note les coefficients sous la forme, $c_1 = \gamma_1 e^{i\varphi_1}$ et $c_2 = \gamma_2 e^{i\varphi_2}$, on obtient de la sorte une approximation de γ_1 et de γ_2 et seules les phases restent indéterminées. En fait, seule la différence de phase, φ_2-φ_1, compte car le vecteur d'état global n'est jamais déterminé qu'à une phase inessentielle près. Le même observateur peut tenter de l'estimer en réservant une partie des électrons à une analyse différente, selon Ox cette fois. Dans la base de travail, $|z+\rangle, |z-\rangle$, les vecteurs propres de l'opérateur associé à la composante du spin selon Ox se notent :

$$v_{x+} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \text{ et } v_{x-} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix},$$

d'où on calcule les probabilités de détection des électrons dans les directions x+ et x- :

$$p_{x+} = \left|\langle v_{x+}|\psi\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}c_1\\c_2\end{pmatrix}\right|^2 = \frac{1}{2}\left(\gamma_1^2 + \gamma_2^2 + 2\gamma_1\gamma_2\cos(\varphi_2 - \varphi_1)\right)$$

$$p_{x-} = \left|\langle v_{x-}|\psi\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\end{pmatrix}\begin{pmatrix}c_1\\c_2\end{pmatrix}\right|^2 = \frac{1}{2}\left(\gamma_1^2 + \gamma_2^2 - 2\gamma_1\gamma_2\cos(\varphi_2 - \varphi_1)\right),$$

valeurs que l'on peut à nouveau comparer aux fréquences observées pour en déduire une approximation de la différence de phase.

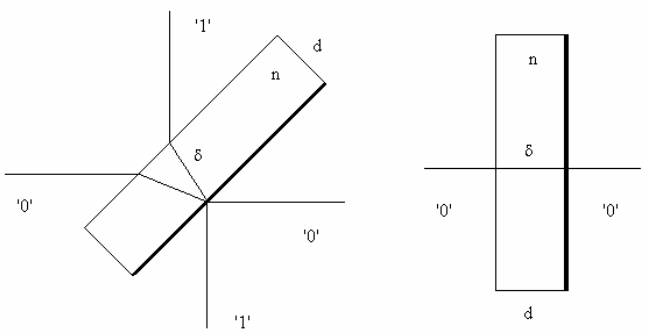
Mais ce procédé ne répond pas du tout à la question posée : à supposer même (ce qui n'est déjà pas le cas) que chaque particule dans le faisceau possède un vecteur d'état objectivable, $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$, il n'y a aucune raison pour que les autres particules adhèrent au même vecteur. Au contraire, le faisceau apparaîtrait tout au plus comme un mélange d'individus aux coefficients tous différents. Tout ce qu'on aurait réussi à faire c'est une étude statistique étendue à un mélange de particules.

C'est toute la différence qui existe entre une source polarisée et une source qui ne l'est pas. Une source polarisée est munie d'un analyseur qui filtre d'office les particules émises dans un état préassigné. Cela se fait évidemment au prix d'une absorption des particules non filtrées. Par exemple, une source lumineuse munie d'un polariseur selon Ox puis d'un polariseur orienté à 45° puis enfin d'une lame quart d'onde est une source polarisée circulairement.

Insistons sur ce fait qu'une statistique précise exige une infinité de mesures. Il est donc impossible, par une procédure finie, de prendre connaissance du vecteur d'état d'une particule. Une conséquence est qu'il est tout aussi impossible de cloner un état inconnu donc d'en fabriquer une copie fidèle sans détruire le modèle, c'est le « No cloning theorem ». Par contre, il est parfaitement possible de préparer une cohorte de clones sur un modèle connu. Par exemple, un appareil de Stern-Gerlach, aligné selon l'axe Oz, prépare autant d'électrons que l'on veut dans un même état de polarisation magnétique, $|0\rangle$ ou $|1\rangle$. De tels états sont dits purs par opposition aux états mélangés de la source non polarisée.

Implémentation physique des portes H et Φ.

Voyons sur un exemple concret comment on peut simuler physiquement le comportement des portes H et Φ.



Dans le cas de la porte H, le vecteur d'état incident, qu'il soit de type '0' ou '1', subit une séparation dictée par la matrice :

$$\begin{pmatrix} e^{in\delta} & e^{2in\delta} \\ -1 & e^{in\delta} \end{pmatrix}$$

où δ représente la longueur de la traversée oblique dans la lame ($\delta = \frac{nd\sqrt{2}}{\sqrt{2n^2-1}}$). Il suffit de choisir convenablement l'épaisseur, d, de la lame, en sorte que l'on ait, $n\delta=2\pi$, et cette matrice s'écrit :

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

L’ordinateur quantique.

Richard Feynman

Charles Bennett

L'ordinateur quantique : pour quoi faire ?

La théorie classique de l'information a été décrite par ailleurs. Elle est basée sur l'existence de la notion de bit, une variable discrète pouvant prendre deux états contrastés, notés '0' et '1'. La notion d'information est aussi fondamentale, en physique, que l'énergie : nous avons vu, dans l'exposé consacré à la thermodynamique, qu'en la reliant intimement à la notion d'entropie, elle lui consacre un principe d'égale importance.

Cette théorie n'est pas seulement un modèle abstrait décrivant la meilleure manière de stocker, de traiter et d'échanger de l'information. Elle présente également de nombreuses applications pratiques qui gravitent toutes dans le domaine de l'informatique appliquée. L'ordinateur joue pour l'information un rôle comparable à celui que le moteur joue vis-à-vis de l'énergie : l'un comme l'autre permettent d'illustrer concrètement le principe de la physique auxquels ils sont étroitement associés.

D'une manière générale, la théorie de l'information ne se préoccupe pas de la propriété physique qui réalise l'encodage des bits au sein d'un système donné, l'ordinateur, par exemple. La physique classique offre, à cet égard, une infinité de possibilités parmi lesquelles les concepteurs de l'ordinateur de l'an 2000 ont dû faire un choix. Ils ont clairement adopté les systèmes à deux états de tension électrique. Aucun modèle alternatif n'est sinon à l'étude, du moins en passe de supplanter rapidement le système transistorisé.

Si l'ordinateur classique existe, avec des performances que nous jugeons acceptables, il a pourtant ses faiblesses :

- Il est terriblement entropogène par rapport à ce qu'exigent les lois de la physique et cela se manifeste par une dissipation excessive de chaleur dans l'environnement. Ce point a été abondamment discuté dans le chapitre réservé à la thermodynamique du calcul et nous y avons vu un obstacle sérieux à une miniaturisation poussée toujours plus loin.

- Une autre faiblesse est qu'il épouse le schéma de la machine de Turing classique et qu'à ce titre il effectue ses calculs en séquence. La conséquence est qu'il est impuissant à démêler, dans un temps raisonnable, un grand nombre d'instances des problèmes NP.

Feynman fut le premier à réfléchir aux avantages que présenterait la construction d'un ordinateur où l'encodage du bit serait miniaturisé à l'échelle atomique. Naturellement les lois auxquelles obéirait une telle machine seraient les lois quantiques mais précisément il y a vu la possibilité d'optimiser de façon définitive le traitement de l'information.

En encodant l'information au niveau atomique, il est clair qu'on atteint la miniaturisation maximale désirée et que, de plus, on évite les sources de dissipation habituellement liées aux frottements macroscopiques. Mais il y a mieux car nous verrons qu'au niveau du traitement de cette information, les performances de l'ordinateur quantique sont théoriquement très supérieures à celles de l'ordinateur classique : le calcul séquentiel est en effet remplacé par un calcul massivement parallèle qui ouvre, de ce fait, la voie à une résolution rapide des instances ardues des problèmes NP avec toutes les conséquences bouleversantes que cela aurait, en particulier dans le domaine de la cryptographie.

En cette matière, le conditionnel est tout à fait de rigueur car l'ordinateur quantique n'est actuellement guère plus qu'un rêve même si aucune loi connue de la physique n'interdit

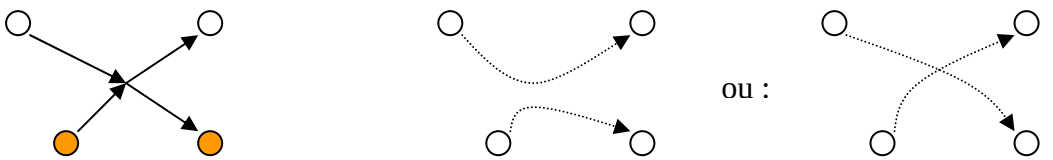
d'espérer le réaliser un jour. Les études théoriques ont bien avancé mais la technologie ne suit pas et il n'est pas du tout certain qu'elle rattrapera un jour son retard. Le problème majeur qui se pose est le revers de la médaille à l'absence de dissipation. Car si les frottements sont souvent ressentis comme une gêne, ils ont aussi leurs beaux côtés : ils sont souvent les garants d'une stabilité bien nécessaire du fait qu'ils offrent une protection naturelle contre les bruits. On peut, par exemple, encoder classiquement un bit en décidant de charger ou non un condensateur sous une tension de 5V. On sait que les charges et décharges successives de ce condensateur entraîneront une dissipation de chaleur dans la résistance de charge mais au moins on a la certitude qu'aucune fluctuation raisonnable de tension due à l'environnement ne viendra jamais fausser l'encodage. On voit bien qu'en passant de 5V à 0.5V, on diminuerait la dissipation mais on augmenterait simultanément, de façon préoccupante, le risque de perturbation externe.

Tout cela cesse d'être vrai à l'échelle quantique où l'absence de dissipation exige l'isolation parfaite du système vis-à-vis de l'environnement et ce problème majeur n'est pas résolu à ce jour. Actuellement, en 2005, on est en mesure de maintenir la cohérence de 6 ou 7 qubits (nom donné aux bits quantiques) maximum alors qu'il en faudrait quelques centaines pour entrer dans le domaine de l'application pointue.

Pour comprendre ce qui différencie l'ordinateur quantique de son homologue classique, il est nécessaire de se remémorer le détail des principes de la mécanique quantique. On se souvient qu'une particularité du qubit isolé, par rapport au bit classique, est de pouvoir exister dans des états de superposition linéaire. Mais il y a plus : lorsqu'on considère simultanément plusieurs qubits confinés, ils sont indiscernables au point d'enchevêtrer (on dit aussi intriquer) leur vecteur d'état commun. C'est assurément la possibilité d'intriquer plusieurs qubits qui rend prometteur le traitement quantique de l'information. En revanche, la fragilité de cette intrication fait que des systèmes quelque peu complexes brisent aisément leur cohérence et rejoignent le monde classique. Précisons en quoi l'intrication est au cœur de la différence de performances entre les ordinateurs classique et quantique. Un détour s'impose par un postulat supplémentaire de la mécanique quantique : le principe d'indiscernabilité.

Le principe d'indiscernabilité.

Une conséquence inattendue du principe d'incertitude concerne l'indiscernabilité des particules identiques. Dans le monde macroscopique, les boules de billard peuvent se ressembler autant que l'on veut, il y a toujours moyen de les suivre à la trace sans perturber leur mouvement de manière appréciable en sorte que lors d'une collision, par exemple, il est parfaitement possible de dire quelle boule entrante sort sous un angle déterminé. Cela n'est plus vrai du tout avec des électrons puisque la notion même de trajectoire a perdu toute signification : le problème n'est pas tant qu'on serait incapable de les « voir » avec une sonde appropriée mais bien que cette sonde chamboulerait complètement leur état.



boules de billard électrons

L'exemple suivant aide à comprendre la différence de comportements des objets classiques et quantiques.

Système planétaire à trois corps. Deux planètes qui gravitent autour d'une même étoile forment un système à trois corps qui possèdent leur individualité propre, que les équations de la mécanique respectent en les traitant séparément. Autrement dit, ce système peut être décomposé en n=3 sous-systèmes auxquelles les lois classiques s'appliquent individuellement. Par exemple on écrirait :

$$m_i \ddot{\vec{r}}_i = G m_i \sum_{j=1,\, j\neq i}^{n} \frac{m_j(\vec{r}_j - \vec{r}_i)}{\left|\vec{r}_j - \vec{r}_i\right|^{3/2}} \qquad (i = 1, \cdots, n).$$

La solution numérique de ce problème peut être calculée en un temps raisonnable par un ordinateur classique. Certes ce système a toutes les chances d'être chaotique mais à condition d'encoder les, 6x3=18, conditions initiales avec une précision suffisante, rien ne s'oppose à ce qu'on prédise l'évolution du système jusqu'à n'importe quel temps t, fixé d'avance. La solution du même problème, à n>3 corps cette fois, prendrait sans doute plus de temps car le nombre des variables passerait de 6x3 à 6xn mais le fait est que ce temps resterait raisonnable et en tous cas accessible à un ordinateur classique. Au fond, ce qui rend le problème classique à n corps abordable (pour n raisonnablement modéré), c'est le fait que la dimension de l'espace vectoriel nécessaire à sa résolution ne croît que comme une puissance (ici la première puissance) du nombre n. En effet, le produit cartésien des espaces de phases de chacun des n corps ne comporte que 6xn dimensions au total.

L'atome d'hélium. Deux électrons prisonniers d'un noyau d'hélium forment également un système à trois corps, quantique cette fois. La grande différence est que ces électrons sont totalement indiscernables : ils forment un système intriqué. Leur vecteur d'état, $|\psi\rangle = |\psi(v_1, v_2, t)\rangle$, où les v_i abrègent la notation des variables externes de position et internes de spin, doit certainement traduire quelque part cette indifférence à toute tentative de numérotation des particules individuelles. Nous savons que ce vecteur d'état évolue conformément à la loi,

$$i\hbar\partial_t |\psi\rangle = H(v_1, v_2)|\psi\rangle .$$

Même en se contentant d'étudier les seuls états stationnaires, qui obéissent à l'équation volontairement simplifiée, où l'on ignore toute contribution de spin,

$$H(\vec{r}_1, \vec{r}_2)|\psi\rangle = -\frac{\hbar^2}{2m}(\Delta_1 + \Delta_2)|\psi\rangle + V(\vec{r}_1, \vec{r}_2)|\psi\rangle = E|\psi\rangle,$$

on peut montrer que cette équation aux 6 (!) dérivées partielles ne constitue généralement pas un problème bien posé : elle possède, en fait, une infinité de solutions appartenant toutes à L_2. Autrement dit, l'ensemble des principes de la mécanique quantique tels qu'ils ont été énoncés dans la première partie, ne suffit pas à définir une solution unique au problème posé par les systèmes de particules identiques.

On peut s'en convaincre plus aisément sur l'exemple simplifié d'un système de deux particules identiques soumises à une interaction additive du type, $V(\vec{r}_1, \vec{r}_2) = V_1(\vec{r}_1) + V_2(\vec{r}_2)$.

Dans ce cas, il est certainement possible de trouver une solution acceptable, ($\in L_2$), s'écrivant sous la forme séparable, $|\psi(\vec{r}_1,\vec{r}_2)\rangle = |\psi_1(\vec{r}_1)\rangle \otimes |\psi_2(\vec{r}_2)\rangle$. Mais alors, il vient immédiatement que $|\psi(\vec{r}_1,\vec{r}_2)\rangle = |\psi_1(\vec{r}_2)\rangle \otimes |\psi_2(\vec{r}_1)\rangle$ est également solution, d'où n'importe quelle combinaison linéaire des deux l'est aussi :

$$|\psi(\vec{r}_1,\vec{r}_2)\rangle = \lambda_1 |\psi_1(\vec{r}_1)\rangle \otimes |\psi_2(\vec{r}_2)\rangle + \lambda_2 |\psi_1(\vec{r}_2)\rangle \otimes |\psi_2(\vec{r}_1)\rangle .$$

Or rien dans les principes généraux de la mécanique quantique ne permet de choisir la « bonne » solution parmi toutes celles que l'on vient d'écrire. Autrement dit, il manque un principe qui réduit les solutions acceptables à une seule.

L'observation suivante guide le choix de ce principe supplémentaire : le hamiltonien ne peut faire aucune différence entre deux particules indiscernables d'où il est nécessairement symétrique par rapport à l'échange des variables, v_1 et v_2 :

$$H(v_1, v_2) = H(v_2, v_1) .$$

On pose en principe, dit de symétrisation, que le vecteur d'état associé à un système de n particules indiscernables est obligatoirement soit totalement symétrique soit totalement antisymétrique par rapport à toute permutation dans la numérotation des particules. Cela donnerait deux possibilités, dans le cas particulier d'un potentiel additif, (n=2) :

1) $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\psi_1(v_1)\rangle \otimes |\psi_2(v_2)\rangle + |\psi_1(v_2)\rangle \otimes |\psi_2(v_1)\rangle\right)$, si les particules sont de spin demi-entier (fermions, ce sont les particules de matière, électron, nucléons, …) et plus généralement, si le potentiel est quelconque : $|\psi(v_1, v_2\rangle = |\psi(v_2, v_1\rangle$.

2) $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\psi_1(v_1)\rangle \otimes |\psi_2(v_2)\rangle - |\psi_1(v_2)\rangle \otimes |\psi_2(v_1)\rangle\right)$, si les particules sont de spin entier (bosons, ce sont les particules médiatrices d'interaction entre fermions, photons, pions, …) et plus généralement : $|\psi(v_1, v_2\rangle = -|\psi(v_2, v_1\rangle$.

Remarque : la notation, v_i, regroupe les variables d'espace et de spin. Une particule dénuée de spin se verrait attribuer un vecteur d'état scalaire et dans ce cas simple le principe de symétrie ne porterait que sur les variables d'espace. Dès que la particule est spinale, son vecteur d'état évolue dans l'espace de Hilbert résultant du produit extérieur des deux sous-espaces correspondants aux variables externes et internes. Dans une représentation matricielle, on écrirait :

$$|\psi(v_1, v_2)\rangle = c_1(\vec{r}_1,\vec{r}_2)|0\rangle + c_2(\vec{r}_1,\vec{r}_2)|1\rangle = \begin{pmatrix} c_1(\vec{r}_1,\vec{r}_2) \\ c_2(\vec{r}_1,\vec{r}_2) \end{pmatrix}.$$

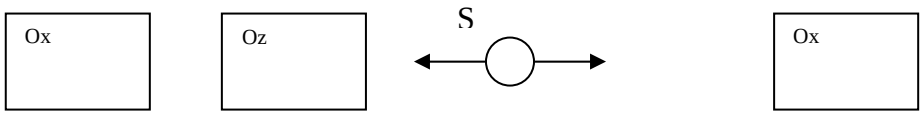
Dans ce cas, c'est le vecteur d'état global qui est soumis au principe de symétrie :

$$\begin{pmatrix} c_1(\vec{r}_1,\vec{r}_2) \\ c_2(\vec{r}_1,\vec{r}_2) \end{pmatrix} = + \begin{pmatrix} c_2(\vec{r}_2,\vec{r}_1) \\ c_1(\vec{r}_2,\vec{r}_1) \end{pmatrix} \qquad \text{(bosons)}$$

ou

$$\begin{pmatrix} c_1(\vec{r}_1,\vec{r}_2) \\ c_2(\vec{r}_1,\vec{r}_2) \end{pmatrix} = + \begin{pmatrix} c_2(\vec{r}_2,\vec{r}_1) \\ c_1(\vec{r}_2,\vec{r}_1) \end{pmatrix} \qquad \text{(fermions).}$$

Le principe de symétrie vient s'ajouter aux principes de base déjà énoncés. A ce titre, il ne se démontre pas mais on le crédibilise grâce à l'expérience suivante. Considérons une source, S, de spin nul, n'ayant fait l'objet d'aucune préparation particulière, qui émet en opposition deux particules de spins 1/2, nécessairement opposés afin de satisfaire la loi de conservation du moment angulaire.



En l'absence de toute mesure de spin, le système des deux particules, numérotées 1 et 2, est intriqué et il peut être décrit par le vecteur d'état :

$$|\psi\rangle = \alpha|z+\rangle_1|z-\rangle_2 + \beta|z-\rangle_1|z+\rangle_2 \qquad (|\alpha|^2 + |\beta|^2 = 1).$$

On cherche une procédure expérimentale capable de révéler les valeurs des coefficients α et β. Imaginons, à cet effet, que nous analysions la particule émise à gauche par un appareil de Stern-Gerlach orienté selon Oz : on trouve +1/2 et –1/2 en moyenne une fois sur deux. Ceci indique que, $|\alpha|^2 = |\beta|^2 = 1/2$, donc que le vecteur d'état devait s'écrire, à une phase globale inessentielle près :

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 + e^{i\varphi}|z-\rangle_1|z+\rangle_2\right).$$

A ce stade, la phase résiduelle, φ, demeure inconnue. Plaçons à présent, symétriquement, deux analyseurs orientés selon Ox de telle manières qu'ils soient traversés après le premier et voyons avec quelle probabilité, $P_{++,x}$, les mesures, effectuées selon Ox, donneraient le même résultat, +1/2, tant à gauche qu'à droite de la source. L'expérience indique qu'avec des électrons cette probabilité est nulle, $P_{++,x} = 0$. Or le calcul de $P_{++,x}$ donne :

$$P_{++,x} = \left|{}_1\langle x+|{}_2\langle x+|\psi\rangle\right|^2 = \left|{}_1\langle x+|{}_2\langle x+|\frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 + e^{i\varphi}|z-\rangle_1|z+\rangle_2\right)\right|^2$$

$$= \left|{}_1\langle x+|{}_2\langle x+|\frac{1}{2\sqrt{2}}\left((|x+\rangle_1 - |x-\rangle_1)(|x+\rangle_2 + |x-\rangle_2) + e^{i\varphi}(|x+\rangle_1 + |x-\rangle_1)(|x+\rangle_2 - |x-\rangle_2)\right)\right|^2$$

$$= \frac{1}{2}\cos^2\frac{\varphi}{2}$$

d'où on conclut que, $\varphi = \pi$, et que le vecteur d'état des électrons émis par la source est antisymétrique :

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 - |z-\rangle_1|z+\rangle_2\right).$$

Nous verrons sous peu qu'une expérience similaire conduite avec des photons et des polariseurs en lieu et place d'appareils de Stern-Gerlach donnerait un résultat différent : la probabilité, $P_{++,x}$, serait égale à 1/2 d'où la phase φ serait nulle et le vecteur d'état symétrique,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 + |z-\rangle_1|z+\rangle_2\right).$$

L'intrication du vecteur d'état a une conséquence dramatique sur le calcul des états d'un atome possédant n électrons : il n'est plus possible de considérer séparément chaque électron comme on le fait classiquement avec des planètes. La mécanique quantique traite ses problèmes dans des espaces de Hilbert dont le nombre de degrés de libertés augmente exponentiellement en fonction du nombre n de corps présents. Techniquement parlant, cela résulte du fait que l'espace de Hilbert global est le produit tensoriel (et non plus cartésien) des espaces individuels.

Envisageons plus concrètement un atome à n électrons. Il est décrit par une fonction d'onde obéissant à l'équation de Schrödinger, dont l'amplitude dépend de toutes les variables de position (on néglige les corrections de spin qui ne feraient qu'aggraver la situation) :

$$\psi = \psi(\vec{r}_1, \vec{r}_2, \cdots, \vec{r}_n).$$

En réalité, les n électrons sont indiscernables en sorte que la fonction d'onde doit, en fait, être antisymétrique pour toutes permutations des particules. Or la fonction d'onde d'un système de n particules identiques s'écrit comme une somme de n ! fonctions du type :

$$\psi_{antisym} = \frac{1}{\sqrt{n!}}\sum_{\forall perm}(-1)^{sign}\psi(\vec{r}_{i1}, \vec{r}_{i2}, \vec{r}_{i3}, \cdots, \vec{r}_{in}).$$

Lorsque n augmente cette fonction devient rapidement ingérable pour un ordinateur classique. Rien que l'écriture d'un bout de programme calculant l'atome de fer (26 électrons) exigerait d'y inscrire une fonction d'onde combinant la bagatelle de 26 ! = 4.10^{26} fonctions individuelles. Ce n'est pas irréalisable en théorie mais c'est totalement irréaliste. Insistons, il ne s'agit nullement d'une incapacité fondamentale à régler le problème : rien n'empêcherait l'ordinateur classique de calculer l'atome de fer, si on le voulait, car son principe repose sur

celui d'une machine de Turing universelle et le propre d'une MTU est d'être capable de calculer tout ce qui est calculable. L'incapacité se situe au niveau du temps de calcul qui dépasserait largement l'âge de l'univers, sans parler de l'encombrement de la mémoire.

Au fond, cette croissance dramatique en fonction de n est typique des problèmes NP : nous avons vu, dans le chapitre réservé à la calculabilité, que lorsqu'on tente une résolution du problème du voyageur de commerce par la méthode exhaustive on se heurte également à un nombre d'éventualités à prendre en considération de l'ordre de n !

Pourtant la nature calcule l'évolution, en temps réel, de tous ses atomes même les plus compliqués ! Si l'on pose, comme on le fait en physique classique, qu'un système quantique, tel un atome de béryllium, est équivalent à une MT (quantique) particulière dédicacée précisément au calcul de sa propre évolution en temps réel, la supériorité de la machine quantique saute aux yeux. Evidemment un atome de béryllium n'est pas équivalent à une MTU mais on verra que le concept de MTU reste valable dans le monde quantique et qu'en s'y prenant adroitement on peut, au moins en théorie, espérer l'implémenter un jour physiquement sous la forme d'un véritable ordinateur quantique.

Opérations logiques élémentaires sur le qubit isolé.

Nous avons appris comment préparer un qubit isolé dans un état de superposition arbitrairement donné : seules sont nécessaires les portes de Hadamard et de déphasage. Une fois le qubit préparé quel genre de traitement arithmético-logique peut-on imaginer lui faire subir ? Dans le cas du bit classique la réponse est simple, il n'y en a que deux : l'identité (Id) et la négation (Not). Les transformations unitaires qui effectuent les mêmes opérations sur le qubit isolé possèdent les représentations matricielles suivantes :

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \mathrm{Not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On vérifie qu'elles conservent le nombre de '0' et de '1' :

$$\text{Exemple : } \mathrm{Not}(c_1|0\rangle + c_2|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} c_2 \\ c_1 \end{pmatrix} = (c_2|0\rangle + c_1|1\rangle).$$

On peut proposer une autre notation, plus compacte, qui se révélera utile pour la suite :

$$\mathrm{Id} = |0\rangle\langle 0| + |1\rangle\langle 1| \qquad \text{et} \qquad \mathrm{Not} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

et on vérifie sans peine que ces opérateurs appliqués à $|0\rangle$ ou $|1\rangle$ effectuent l'opération attendue.

Le qubit isolé autorise d'autres transformations unitaires dont certaines effectuent des opérations fort peu intuitives. Ainsi la transformation, SqNot, notée comme suit :

$$\mathrm{SqNot} = \frac{e^{i\pi/4}}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}.$$

On vérifie que : $\mathrm{SqNot}^2 = \mathrm{Not}$. En d'autres termes, la même opération effectuée deux fois de suite équivaut à la négation. C'est un exemple d'une performance impossible à réaliser en théorie classique de l'information.

On rappelle que les portes de déphasage, Φ, et de Hadamard, H, forment un couple universel pour les transformations unitaires du qubit isolé. Il doit donc être possible de réduire SqNot à un assemblage de ces deux portes. De fait, on vérifie que trois portes suffisent :

$$\mathrm{SqNot} = e^{i\pi/4}\Phi(-\pi/2)\mathrm{H}\Phi(-\pi/2).$$

Registres de n qubits.

Le qubit isolé ne mène pas très loin en théorie de l'information. Un ensemble de n (qu)bits, s'appelle un registre. Un registre classique de n bits peut stocker 2^n messages différents mais il ne peut en stocker qu'un seul à la fois. Un registre quantique peut faire beaucoup mieux car la superposition quantique lui permet de les stocker tous en même temps. Naturellement, lorsqu'on cherche à prendre connaissance du contenu du registre, l'acte de mesure ne peut révéler qu'un seul message sélectionné au hasard. Ce sera tout l'art de la programmation quantique de tirer parti du bénéfice sans pâtir de la limitation.

L'écriture des contenus possibles d'un registre soulève un problème de notations. Par exemple, si n=2, 4 messages distincts sont autorisés. Une première manière de les noter consiste à les prendre dans l'ordre arithmétique, $(|0\rangle,|1\rangle,|2\rangle,|3\rangle)$. Dans cette optique, l'encodage se fait sur base d'un produit tensoriel en respectant l'ordre binaire et on écrit indifféremment :

$$\begin{aligned}
|0\rangle &\equiv |00\rangle_{AB} \equiv |0\rangle_A \otimes |0\rangle_B \equiv |0\rangle_A|0\rangle_B \\
|1\rangle &\equiv |01\rangle_{AB} \equiv |0\rangle_A \otimes |1\rangle_B \equiv |0\rangle_A|1\rangle_B \\
|2\rangle &\equiv |10\rangle_{AB} \equiv |1\rangle_A \otimes |0\rangle_B \equiv |1\rangle_A|0\rangle_B \\
|3\rangle &\equiv |11\rangle_{AB} \equiv |1\rangle_A \otimes |1\rangle_B \equiv |1\rangle_A|1\rangle_B
\end{aligned}.$$

Les indices A et B ne sont pas indispensables mais ils aident à se remémorer que les vecteurs indicés différemment évoluent dans des espaces distincts. En particulier, les relations d'orthonormation ne concernent que les vecteurs de mêmes indices :

$${}^A\langle 0|0\rangle_A = {}^A\langle 1|1\rangle_A = {}^B\langle 0|0\rangle_B = {}^B\langle 1|1\rangle_B = 1 \qquad {}^A\langle 0|1\rangle_A = {}^A\langle 1|0\rangle_A = {}^B\langle 0|1\rangle_B = {}^B\langle 0|1\rangle_B = 0.$$

On peut généraliser la représentation matricielle au cas des registres mais l'agrément qu'elle procure est tempéré par le fait qu'en général, le produit tensoriel de deux vecteurs de dimensions m_1 et m_2 est de dimension m1xm2. Même pour des dimensions modérées, la notation matricielle devient rapidement encombrante. Par exemple dans le cas n=2, on a les quatre vecteurs de base de l'espace de Hilbert où le registre évolue :

$$|0\rangle_A \otimes |0\rangle_B = \begin{pmatrix}1\\0\end{pmatrix}_A \otimes \begin{pmatrix}1\\0\end{pmatrix}_B = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |0\rangle_A \otimes |1\rangle_B = \begin{pmatrix}1\\0\end{pmatrix}_A \otimes \begin{pmatrix}0\\1\end{pmatrix}_B = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|1\rangle_A \otimes |0\rangle_B = \begin{pmatrix}0\\1\end{pmatrix}_A \otimes \begin{pmatrix}1\\0\end{pmatrix}_B = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad |1\rangle_A \otimes |1\rangle_B = \begin{pmatrix}0\\1\end{pmatrix}_A \otimes \begin{pmatrix}0\\1\end{pmatrix}_B = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Les indices A et B sont très utiles lorsqu'on passe aux opérateurs. Il est, en effet, ambigu de déclarer soumettre un registre comprenant deux qubits à l'opération Not tant qu'on ne précise pas si cet opérateur s'applique à A, à B ou aux deux simultanément. Les représentations matricielles sont évidemment différentes dans chaque cas. On a en effet, selon le cas :

$$\mathrm{Not}_A \otimes \mathrm{Id}_B = \begin{pmatrix}0&1\\1&0\end{pmatrix}_A \otimes \begin{pmatrix}1&0\\0&1\end{pmatrix}_B = \begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix},$$

$$\mathrm{Id}_A \otimes \mathrm{Not}_B = \begin{pmatrix}1&0\\0&1\end{pmatrix}_A \otimes \begin{pmatrix}0&1\\1&0\end{pmatrix}_B = \begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix},$$

$$\mathrm{Not}_A \otimes \mathrm{Not}_B = \begin{pmatrix}0&1\\1&0\end{pmatrix}_A \otimes \begin{pmatrix}0&1\\1&0\end{pmatrix}_B = \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}.$$

On voit que l'encombrement de la notation matricielle augmente quand on passe aux opérateurs. Cela est bien naturel puisque le produit tensoriel entre opérateurs de dimensions (m_1, n_1) et (m_2, n_2) est lui-même de dimension $m_1m_2xn_1n_2$.

La représentation matricielle des opérateurs devient progressivement ingérable dès que le nombre des qubits du registre excède 2 : il faudrait travailler dans un espace de dimension

2^n. Dans ce cas, seule la notation tensorielle est concevable mais elle requiert du soin dans la gestion des indices, A, B, C, … . On aurait par exemple :

$$\mathrm{Not}_A = |0\rangle_A {}^A\langle 1| + |1\rangle_A {}^A\langle 0| \qquad \text{et} \qquad \mathrm{Not}_B = |0\rangle_B {}^B\langle 1| + |1\rangle_B {}^B\langle 0|,$$

d'où on écrit :

$$\mathrm{Not}_A \otimes \mathrm{Not}_B = \left(|0\rangle_A {}^A\langle 1| + |1\rangle_A {}^A\langle 0|\right)\left(|0\rangle_B {}^B\langle 1| + |1\rangle_B {}^B\langle 0|\right).$$

Quelle que soit la notation retenue, on vérifie que l'on a bien, par exemple :

$$\left(\mathrm{Not}_A \otimes \mathrm{Not}_B\right)\left(|0\rangle_A \otimes |1\rangle_B\right) = |1\rangle_A \otimes |0\rangle_B.$$

Préparation d'un registre de n qubits.

Préparer un registre dans un état donné est plus compliqué que pour le qubit isolé. L'opération n'est simple que si l'état est séparable : on veut dire par là que le vecteur d'état est complètement factorisable par rapport aux n qubits qui le composent, ce que traduit la notation,

$$|\psi_{sep}\rangle = \bigotimes_{i=1}^{n}\left(\alpha_i|0_i\rangle + \beta_i|1_i\rangle\right).$$

Pour préparer un tel état séparable, on procède en deux temps comme dans le cas du qubit isolé. On commence par le préparer dans un état de base, disons $|000\cdots 0\rangle$, en filtrant chaque qubit du registre dans l'état correspondant, $|0\rangle$. Ensuite, on applique, en parallèle, la transformation, U(θ,φ), à chaque qubit :

$|0\rangle_A$ —□—◇—□—◇— $e^{i\theta_A/2}(\cos(\theta_A/2)|0\rangle_A + e^{i\varphi_A}\sin(\theta_A/2)|1\rangle_A)$

$|0\rangle_B$ —□—◇—□—◇— Idem(B)

$|0\rangle_C$ —□—◇—□—◇— Idem (C)

L'état de superposition d'un registre peut être plus ou moins complet, ainsi :

- l'état, $|000\rangle$, n'est pas superposé, c'est un état de base élargie à l'espace du registre,
- l'état, $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\otimes|1\rangle\otimes|1\rangle = \frac{1}{\sqrt{2}}\left(|011\rangle + |111\rangle\right) = \frac{1}{\sqrt{2}}\left(|3\rangle + |7\rangle\right)$, est partiellement superposé,
- enfin l'état,

$$\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)=$$
$$\frac{1}{\sqrt{8}}\left(|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle+|101\rangle+|110\rangle+|111\rangle\right)=$$
$$\frac{1}{\sqrt{8}}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle\right)$$

est maximalement superposé.

Cependant, la plupart des états de registres ne sont pas séparables. Dans l'exemple, n=3, l'état noté,

$$|\psi_{int}\rangle=\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right),$$

n'est manifestement pas séparable car il est impossible de l'écrire sous la forme d'un produit tensoriel de trois facteurs, un par qubit. Un tel état est dit intriqué (ou enchevêtré). Plus généralement, l'état,

$$\psi=c_1|000\rangle+c_2|001\rangle+c_3|010\rangle+c_4|011\rangle+c_5|100\rangle+c_6|101\rangle+c_7|110\rangle+c_8|111\rangle \qquad \left(\sum_{i=1}^{8}|c_i|^2=1\right)$$

est intriqué s'il est impossible de le factoriser sous la forme,

$$|\psi_{int}\rangle\neq\overset{3}{\underset{i=1}{\otimes}}\left(\alpha_i|0_i\rangle+\beta_i|1_i\rangle\right).$$

Cela se produit toutes les fois que le polynôme,

$$c_1u_1u_2u_3+c_2u_1u_2v_3+c_3u_1v_2u_3+c_4u_1v_2v_3+c_5v_1u_2u_3+c_6v_1u_2v_3+c_7v_1v_2u_3+c_8v_1v_2v_3,$$

est lui même incomplètement factorisable en monômes.

Il existe un critère dû à Schmidt qui permet de décider si un état est séparable ou non. Bien que cela déborde d'un cadre élémentaire, montrons, sans justification, comment il fonctionne. On considère l'état normalisé d'un registre à deux qubits :

$$|\psi\rangle_{AB}=\alpha|0\rangle_A|0\rangle_B+\beta|0\rangle_A|1\rangle_B+\gamma|1\rangle_A|0\rangle_B+\delta|0\rangle_A|0\rangle_B \qquad (|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1),$$

pour quelles valeurs des coefficients est-il séparable ? La réponse s'obtient en calculant la représentation matricielle, dans l'espace B (ou dans l'espace A, au choix) de la trace, ρ, dans l'espace A (dans l'espace B), du projecteur, $|\psi\rangle_{AB}{}^{AB}\langle\psi|$. On trouve dans l'exemple retenu :

$$\rho=$$
$$Tr_A[(\alpha|0\rangle_A|0\rangle_B+\beta|0\rangle_A|1\rangle_B+\gamma|1\rangle_A|0\rangle_B+\delta|0\rangle_A|0\rangle_B)(\alpha^{*A}\langle0|^B\langle0|+\beta^{*A}\langle0|^B\langle1|+\gamma^{*A}1^B\langle0|+\delta^{*A}\langle1|^B\langle1|)]$$

On calcule cette quantité dans le sous-espace, A, en tenant compte de ce que :

La trace de : $|0\rangle_A {}^A\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}(1 \quad 0) = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$ vaut 1,

celle de : $|0\rangle_A {}^A\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}(0 \quad 1) = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$ vaut 0,

celle de : $|1\rangle_A {}^A\langle 0| = \begin{pmatrix}0\\1\end{pmatrix}(1 \quad 0) = \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}$ vaut 0,

enfin celle de : $|1\rangle_A {}^A\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}(0 \quad 1) = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$ vaut 1.

On trouve sans difficultés :

$$\rho = \begin{pmatrix} |\alpha|^2 + |\gamma|^2 & \alpha\beta^* + \gamma\delta^* \\ \alpha^*\beta + \gamma^*\delta & |\beta|^2 + |\delta|^2 \end{pmatrix}.$$

Le nombre de valeurs propres non nulles de ρ s'appelle le nombre de Schmidt de l'état, $|\psi\rangle_{AB}$. Quelle que soit la valeur de n, on a que l'état est intriqué dès que deux valeurs propres, au moins, sont différentes de zéro, sinon il est séparable. Dans l'exemple, l'équation aux valeurs propres se simplifie en :

$$\lambda^2 - \lambda + |\alpha\delta - \beta\gamma|^2 = 0,$$

et la séparabilité exige : $\alpha\delta - \beta\gamma = 0$. La plupart du temps, cette condition ne sera pas satisfaite d'où il résulte que les états intriqués sont beaucoup plus nombreux que les états séparables.

Certes, dans cet exemple, n ne vaut que 2 et on aurait pu déduire ce résultat plus simplement en identifiant les coefficients de l'état donné à ceux de la forme séparable la plus générale, $|\psi_{sep}\rangle = \bigotimes_{i=1}^{n}(\alpha_i|0_i\rangle + \beta_i|1_i\rangle)$, mais la procédure exposée présente l'avantage de rester effective pour les valeurs de n supérieures à 2.

Intrication logique d'un registre à deux qubits.

Les arguments développés montrent que l'encodage de tous les messages possibles sur n qubits, tous coefficients confondus, passent par l'intrication du registre. La question reste posée de savoir s'il existe des portes logiques quantiques capables de préparer des états intriqués à partir des états de base, et, dans l'affirmative, s'il est possible de les implémenter physiquement. Les deux réponses sont positives mais dans un premier temps nous ne considérons que la première.

Rappelons que les portes, H et $\Phi(\varphi)$, suffisent pour préparer n'importe quel registre sous forme séparable. Une seule porte supplémentaire est nécessaire pour passer de la superposition à l'intrication, la porte controlled-Not (cNot). Celle-ci agit sur deux qubits d'entrée qu'elle soumet à la transformation logique :

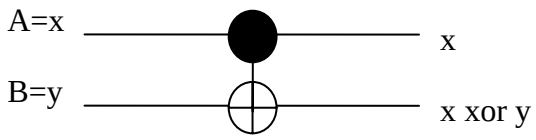
$$\text{cNot}|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle .$$

Dans cette relation, le premier ket apparaît comme un qubit de contrôle et le deuxième est la cible. Le qubit de contrôle n'est pas altéré par la porte logique et la cible ne l'est que si le contrôle vaut '1'. Voici une manière équivalente mais plus explicite d'exprimer les choses :

$$\text{cNot}|0\rangle|y\rangle = |0\rangle|y\rangle$$
$$\text{cNot}|1\rangle|y\rangle = |1\rangle|\neg y\rangle$$

Les représentations matricielle, graphique et tensorielle de la porte cNot s'écrivent respectivement (dans la représentation graphique, le cercle noir signifie que le bit situé à sa gauche est un bit de contrôle) :

$$\text{cNot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



$$\text{cNot}_{AB} = |0\rangle_A {}^A\langle 0| \otimes \text{Id}_B + |1\rangle_A {}^A\langle 1| \otimes \text{Not}_B .$$

Quelle que soit la notation retenue, on vérifie que cNot appliquée à $|1\rangle_A|0\rangle_B$, par exemple, fournit à la sortie, $|1\rangle_A|1\rangle_B$, comme il se doit.

En préparant la cible, B, dans l'état logique '0', on voit que la porte cNot réalise la copie exacte d'un état de base encodé au niveau du qubit de contrôle. On a, en effet :

$$\text{cNot}_{AB}|x\rangle_A|0\rangle_B = |0\rangle_A {}^A\langle 0|x\rangle_A|0\rangle_B + |1\rangle_A {}^A\langle 1|x\rangle_A|1\rangle_B = |x\rangle_A|x\rangle_B \qquad (x = 0,1) .$$

Bref retour au théorème de non-clonage.

On pourrait penser avoir trouvé avec la porte c-Not le moyen de cloner un état donné mais il est facile de voir que cette copie ne fonctionne que sur les états de base, $|0\rangle$ et $|1\rangle$, et pas du tout sur leur superposition, en effet :

$$\text{cNot}_{AB}(\alpha|0\rangle_A + \beta|1\rangle_A)|0\rangle_B = \alpha|0\rangle_A|0\rangle_B + \beta|1\rangle_A|1\rangle_B ,$$

qui est très différent de la copie espérée :

$$\mathrm{cNot}_{AB}(\alpha|0\rangle_A + \beta|1\rangle_A)|0\rangle_B \neq (\alpha|0\rangle_A + \beta|1\rangle_A)(\alpha|0\rangle_A + \beta|1\rangle_A).$$

C'est un fait général qu'il n'existe aucune porte capable de dupliquer un état quelconque et d'effectuer l'opération,

$$U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle.$$

De fait, si U existait, on pourrait écrire :

$$U(|a\rangle + |b\rangle)|0\rangle = |aa\rangle + |bb\rangle \neq (|a\rangle + |b\rangle)(|a\rangle + |b\rangle).$$

Il importe de comprendre que cette impossibilité ne concerne que le clonage des états inconnus. Cloner des états connus est certainement possible : on ne fait rien d'autre quand on prépare une armada de photon dans un même état de polarisation.

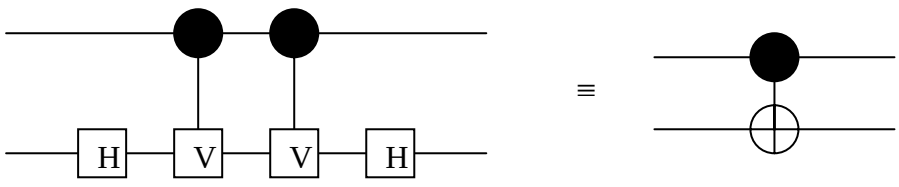
Portes controlled-U.

La porte c-Not est un cas particulier de toute une famille de portes appelées portes controlled-U (c-U), qui fonctionnent sur le même principe : elles conservent toujours le qubit de contrôle et elles n'altèrent la cible, par la transformation unitaire, U, que si le qubit de contrôle vaut '1' :

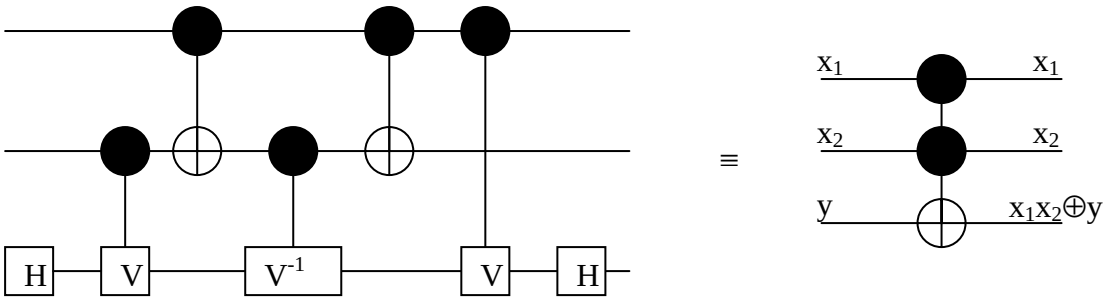
$$\begin{aligned} \mathrm{cU}_{AB}|0\rangle_A|y\rangle_B &= |0\rangle_A|y\rangle_B \\ \mathrm{cU}_{AB}|1\rangle_A|y\rangle_B &= |1\rangle_A|Uy\rangle_B \end{aligned}.$$

La plupart des portes c-U provoquent l'intrication des qubits d'entrée : jointes aux portes H et Φ, elles suffisent dès lors généralement à construire un système universel au sens de Turing. On utilise fréquemment la porte c-V = c-$\Phi(\pi/2)$.

Par exemple, on pourrait construire la porte c-NOT comme suit :



Poursuivant dans la même veine, on observe que quatre portes c-V successives équivalent à l'identité. On en déduit que trois portes c-V successives représentent ensemble l'opération inverse de c-V, que l'on note $(\text{c-V})^{-1}$. Grâce à $(\text{c-V})^{-1}$, on construit la très utile porte controlled-controlled-NOT (cc-NOT), encore appelée porte de Toffoli (T) :



Par convention, toute porte du type, cc-U, ne modifie la cible que si les deux qubits de contrôle valent ‘1’.

Il n’est pas question de proposer une représentation matricielle de la porte de Toffoli, nécessairement 8x8, par contre son écriture tensorielle reste abordable :

$$\mathrm{ccNot}_{ABC} = \mathrm{T} = |0\rangle_A {}^A\langle 0| \otimes \mathrm{Id}_B \otimes \mathrm{Id}_C + |1\rangle_A {}^A\langle 1| \otimes |0\rangle_B {}^B\langle 0| \otimes \mathrm{Id}_C + |1\rangle_A {}^A\langle 1| \otimes |1\rangle_B {}^B\langle 1| \otimes \mathrm{Not}_C .$$

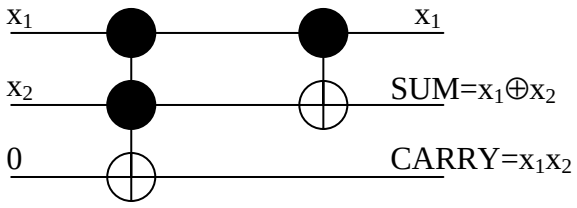
Il existe également une porte « controlled swap », encore appelée porte de Fredkin, F :

$$\mathrm{F} = |0\rangle_A {}^A\langle 0| \otimes \mathrm{Id}_B \otimes \mathrm{Id}_C + |1\rangle_A {}^A\langle 1| \otimes (|00\rangle_{BC} {}^{BC}\langle 00| + |01\rangle_{BC} {}^{BC}\langle 10| + |10\rangle_{BC} {}^{BC}\langle 01| + |11\rangle_{BC} {}^{BC}\langle 11|) .$$

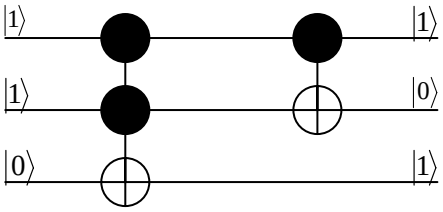
Les portes de déphasage, de Hadamard et c-V forment un ensemble complet pour la manipulation d’un nombre arbitraire de qubits. En garantissant l’universalité au sens de Turing, elles autorisent, en théorie du moins, la construction et l’assemblage des circuits logiques qui composent un ordinateur quantique. L’unitarité de ces portes, qui est inscrite dans les principes mêmes de la mécanique quantique, garantit la réversibilité du calcul.

Implémentation logique de quelques opérations arithmétiques élémentaires.

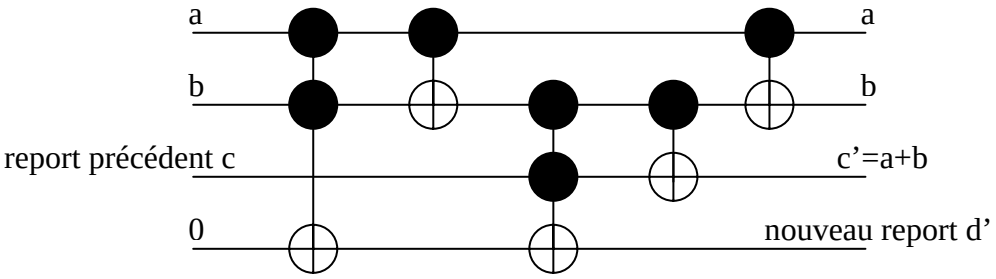
Les portes c-NOT et cc-NOT, correctement agencée, permettent de construire un semi-additionneur (half adder) binaire :



Ce réseau, alimenté par les données, x_1 et x_2, initialisées dans l’un ou l’autre de leurs états logiques, faciles à préparer, $|0\rangle$ ou $|1\rangle$, fournit la réponse au calcul élémentaire posé. Par exemple, l’activation du réseau transforme le registre d’entrée, $|\mathrm{in}\rangle = |110\rangle$, en le registre de sortie, $|\mathrm{out}\rangle = |101\rangle$. Les mesures des qubits 2 et 3 fournissent la somme et le report correspondants à une instance particulière du problème de l’addition de deux chiffres binaires.



On construit un additionneur complet (full adder) sur le même principe. On le nomme ainsi parce qu'il est capable de tenir compte d'un report consécutif à une opération antérieure :



Cahier des charges de l'ordinateur quantique.

La théorie qui précède assemble sur le papier les composantes de l'ordinateur quantique idéal. Elle donne l'illusion trompeuse que sa construction est à portée de main. Cependant l'inventaire des exigences du cahier des charges indique clairement qu'on est encore très loin du compte et les plus pessimistes estiment même qu'un ordinateur quantique digne de ce nom ne verra jamais le jour. Même en mettant les choses au mieux, les premiers ordinateurs quantiques seront à coup sûr dédicacés à quelques tâches particulières et certainement incapables de simuler une machine de Turing universelle. Dans ce sens restrictif, des specimens d'ordinateur quantique existent déjà : un appareil de Stern-Gerlach est un générateur de nombre aléatoire au sens de Kolmogorov, un gaz d'hélium simule son évolution en temps réel et des mesures spectrométriques renseignent immédiatement sur le schéma de ses niveaux énergétiques.

On ne peut plus schématiquement, l'ordinateur quantique part d'une configuration initiale où sont encodées les données du problème posé. Le cas échéant une provision de qubits excédentaires initialisés à '0' sont prévus afin de garantir la réversibilité du calcul. Le système est alors soumis à un hamiltonien variable au cours du temps qui affecte le contenu des registres en simulant le calcul en vue. Cette manœuvre est tellement précise et délicate qu'elle doit être pilotée par un ordinateur classique qui intervient comme auxiliaire de travail. Au terme de l'évolution des registres, la mesure quantique des qubits dédicacés à la sortie du programme renseigne sur la réponse cherchée. L'ordinateur quantique doit rencontrer les exigences suivantes :

- Emprunter une configuration physique à échelle variable (scalable quantum computer). On entend par là que le système physique doit permettre l'encodage d'un nombre arbitrairement grand de qubits. Cette exigence est analogue à l'exigence classique qui concerne toute machine de Turing universelle : la bande de lecture-

écriture doit être de longueur potentiellement infinie. Rappelons que l'on veut dire par là qu'il ne doit pas exister de limitation théorique à l'étendue de la mémoire. Evidemment aucun ordinateur, pas même classique, ne respecte cette exigence au pied de la lettre. Le prix que l'on accepte de payer est l'éventuel plantage de la machine sous l'effet d'un dépassement de capacité mémoire. Cela dit, l'exigence paraît d'autant plus forte à propos de l'ordinateur quantique qu'en 2005 on peine déjà à rassembler un registre de quelques qubits.

- Autoriser la préparation d'un registre dans un état prédéfini. Cette exigence est fondamentale puisque tout calcul quantique passe par l'initialisation du registre dans un état de base, par exemple $|000\cdots0\rangle$. Elle est anodine dans le cas d'un encodage des qubits par des particules en mouvement : un appareil de Stern-Gerlach ou un cristal de calcite sépare physiquement les faisceaux de polarisations différentes en sorte qu'un écran absorbeur suffit à réaliser le filtrage cherché. Mais la même exigence prend des proportions inquiétantes lorsqu'on utilise un encodage par des particules piégées dans une cavité. Sauf à travailler au zéro absolu, l'immersion d'une population de noyaux dans une induction magnétique répartit au hasard les individus en deux classes distinctes dont la population dépend de la température. Il en ressort toutes sortes de complications toutefois surmontables au prix de techniques qui dépassent un exposé élémentaire.

- Réagir à l'influence sélective d'un hamiltonien piloté de l'extérieur du système. Le hamiltonien doit pouvoir garantir un fonctionnement universel au sens de Turing donc au minimum simuler les portes de déphasage, de Hadamard et c-Not. Nous avons vu que tous les modes d'encodage du qubit (électron, états internes ou spatiaux du photon) autorisent sans grand problème les deux premières portes. Si nous n'avons encore rien dit de la porte c-Not, c'est que le problème qu'elle pose est infiniment plus délicat. La raison en est que la porte c-Not exige le concours interactif de deux qubits avec l'environnement. Un peu de réflexion convaincra, en effet, qu'il n'y a rien d'évident à commander un photon d'inverser ou non son état de polarisation selon qu'un autre photon se trouve lui-même dans un état défini : c'est d'autant plus problématique que les photons n'interagissent pas. Le même problème posé avec des électrons ou des noyaux laisse toutefois entrevoir un début de solution : si une induction magnétique extérieure ne peut que piloter un changement d'orientation du moment magnétique, l'interaction spin-spin entre deux particules correctement choisies pourrait peut-être être domestiquée.

- Autoriser un adressage permettant l'interconnection des portes quantiques et la commande sélective du hamiltonien extérieur sur les qubits visés. En informatique classique, cela se fait sans ambiguïté par un assemblage de « fils » dissipatifs mais ce genre d'intermédiaire est précisément absent du monde quantique. De plus, l'indiscernabilité des particules identiques complique singulièrement cet adressage de même qu'il compliquera la lecture des résultats : comment être certain qu'on a manipulé ou lu le « bon » qubit ? En particulier rappelons que la porte c-Not exige la manipulation conjointe et synchronisée de deux qubits imposés.

- Autoriser un mode de lecture des résultats. Il ne suffit pas d'effectuer un calcul, il faut encore pouvoir prendre connaissance de la réponse. Or cela ne peut se faire que via une mesure qui détruit inévitablement, en tout ou en partie, l'intrication des registres en projetant le système, au hasard, sur un seul état propre. Rappelons, sur un exemple

simple, ce que cela signifie. Soit un registre à deux qubits qui a évolué vers l'état généralement intriqué,

$$|\psi\rangle_{AB} = \alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B \qquad (|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1),$$

et supposons qu'une analyse théorique préalable ait révélé que la connaissance du premier qubit, noté, A, suffise à répondre à la question posée. La théorie de la mesure enseigne deux choses :

- que l'on trouvera la valeur 'i' (0 ou 1) avec la probabilité, $p_{A=i}$, valant :

$$p_{A=i} = {}^{AB}\langle\psi|P_{A,i}|\psi\rangle_{AB} = {}^{AB}\langle\psi|\left(|i\rangle_A\,{}^A\langle i|\right)|\psi\rangle_{AB}$$

- que la mesure projettera le registre dans le nouvel état renormalisé,

$$|\psi'\rangle_{AB} = \frac{P_{A,i}|\psi\rangle_{AB}}{|P_{A,i}|\psi\rangle_{AB}|} = \frac{\left(|i\rangle_A\,{}^A\langle i|\right)|\psi\rangle_{AB}}{\left|\left(|i\rangle_A\,{}^A\langle i|\right)|\psi\rangle_{AB}\right|} = \frac{|i\rangle_A\,{}^A\langle i|\psi\rangle_{AB}}{\sqrt{p_{A=i}}}.$$

Par exemple, on trouverait :

$$p_{A=0} = {}^{AB}\langle\psi|P_{A,0}|\psi\rangle_{AB} = {}^{AB}\langle\psi|\left(|0\rangle_A\,{}^A\langle 0|\right)|\psi\rangle_{AB} =$$
$$\left(\alpha^{*\,A}\langle 0|^B\langle 0| + \beta^{*\,A}\langle 0|^B\langle 1| + \gamma^{*\,A}\langle 1|^B\langle 0| + \delta^{*\,A}\langle 1|^B\langle 1|\right)\left(|0\rangle_A\,{}^A\langle 0|\right)\left(\alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B\right)$$
$$= \left(\alpha^{*\,B}\langle 0| + \beta^{*\,B}\langle 1|\right)\left(\alpha|0\rangle_B + \beta|1\rangle_B\right) = |\alpha|^2 + |\beta|^2$$

De même on trouverait,

$$p_{A=1} = |\gamma|^2 + |\delta|^2,$$

d'où une probabilité totale valant naturellement 1. La généralisation à n qubits est immédiate. La plupart du temps (bien qu'il y ait des exceptions), une mesure unique du contenu d'un registre sera incapable de révéler la réponse au problème posé. C'est précisément tout l'art de la programmation quantique que de trouver des algorithmes capables d'extraire le résultat escompté de cette mesure destructrice. Cela implique incontestablement une refonte sérieuse des méthodes de programmation. Plusieurs stratégies sont envisageables : soit on découvre des invariants qui ne dépendent pas de l'état final projeté et qui suffisent à répondre à la question posée soit on recommence le calcul un grand nombre de fois jusqu'à ce qu'une statistique des résultats obtenus suggère avec une forte probabilité une réponse facilement vérifiable.

- Garantir la cohérence du système. Au vu de ce qui précède on voit bien l'ensemble des défis à relever aux niveaux software et hardware. L'informatique quantique théorique ne se préoccupe que de trouver des stratégies capables d'extraire la réponse à un problème posé à partir d'un acte de mesure essentiellement destructeur. C'est déjà un problème redoutable en soi mais il semble que tous les espoirs soient permis : le fait qu'on ait déjà trouvé un algorithme viable pour un problème de la classe NP, à savoir la factorisation des entiers longs, suggère que d'autres progrès sérieux devraient

suivre. L'ingénierie, elle, s'occupe des possibilités d'implémentation et de préservation des registres. Il est clair que sans hardware, l'ordinateur quantique n'est qu'une fiction. Il existe cependant des cas où le software peut voler au secours d'un hardware déficient : c'est le cas toutes les fois que le système corrompt une partie de l'information pour quelques raisons que ce soit et elles ne manquent pas ! On envisage sérieusement de ne pas trop s'en inquiéter et de tolérer un certain pourcentage d'erreurs quitte à démultiplier, par 10 ou par 100 (!), le nombre de qubits au travers d'un système pensé de correction d'erreurs.

Voyons à présent un exemple d'implémentation effectivement à l'étude. En 2005, le seul modèle modestement effectif est basé sur la technologie NMR (nuclear magnetic resonance). Le record, peut-être provisoire, date de 2001 et a vu Isaac Chuang et une équipe d'IBM réussir à coordonner le fonctionnement d'un registre de 7 qubits. Le principe suivant n'est donné qu'à titre indicatif car rien ne permet de penser que le modèle puisse s'étendre aux grands registres.

Considérons le proton d'un atome d'hydrogène ou plus généralement un noyau pourvu d'un moment magnétique, μ, de l'ordre du magnéton nucléaire ($1\mu_N = 5.05\ 10^{-27}$ J/T). Bien que mille fois plus faible que celui de l'électron ce moment est parfaitement mesurable avec une précision qui dépasse 10^{-6}. Si on enferme ce noyau dans une cavité où règne une induction magnétique uniforme, orientée selon Oz pour simplifier, il oriente son spin au hasard selon l'une des deux directions, $|z-\rangle$ ou $|z+\rangle$. Chaque direction correspond à un état énergétique particulier :

- le noyau décrit par le vecteur d'état, $|z-\rangle$, se trouve dans l'état fondamental d'énergie, $E_0 = -\mu B_z$,
- le noyau décrit par le vecteur d'état, $|z+\rangle$, se trouve dans l'état excité d'énergie, $E_1 = +\mu B_z$.

On peut utiliser cette dichotomie pour encoder un qubit : il suffit d'utiliser les deux états (nécessairement orthogonaux puisque états propres d'un hamiltonien hermitien) comme état de base de l'espace de Hilbert correspondant :

$$|z-\rangle = |0\rangle \qquad \text{et} \qquad |z+\rangle = |1\rangle .$$

Dans ce modèle, on peut imaginer préparer un qubit dans l'état, $|z-\rangle = |0\rangle$, en soumettant le noyau à une induction statique suffisamment intense orientée selon Oz et en abaissant la température au voisinage du zéro absolu. On peut ensuite diminuer le champ jusqu'à zéro sans perturber l'état préparé. Si l'on impose ultérieurement une induction faisant un angle quelconque avec la précédente, on réalise une mesure quantique qui a pour effet de projeter l'ancien état sur la nouvelle direction, Oz'. Nous avons appris comment calculer les probabilités de transition, $p[|z-\rangle \to |z'+\rangle]$ et $p[|z-\rangle \to |z'-\rangle]$.

A part l'inconfort de la manœuvre requise par l'abaissement de température, rien n'est nouveau par rapport aux modes d'encodages déjà étudiés. Par contre, le problème traditionnellement posé par l'indiscernabilité des qubits trouve ici une solution naturelle : il suffit de considérer n noyaux magnétiques situés en autant de sites inéquivalents d'une

molécule. Vu que l'environnement physique donc les états énergétiques de chacune diffèrent, il devient possible de piloter le changement d'état d'un qubit particulier. Voici comment on pourrait simuler les portes de Hadamard et de déphasage.

Considérons un noyau dans l'état initial (t = 0),

$$|\psi(0)\rangle = c_0(0)|0\rangle + c_1(0)|1\rangle = \begin{pmatrix} c_0(0) \\ c_1(0) \end{pmatrix}.$$

En l'absence d'induction magnétique extérieure, les deux états de base, $|0\rangle$ et $|1\rangle$, sont caractérisés par des énergies égales à zéro et le vecteur d'état n'évolue pas.

Si on soumet le noyau à une induction magnétique constante d'orientation quelconque, la situation change radicalement : la dégénérescence des niveaux énergétiques est levée et le vecteur d'état évolue en conformité avec l'équation de Schrödinger :

$$i\hbar\partial_t \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = -\mu_p \begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix} \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix}.$$

Sa solution est immédiate :

$$|\psi(t)\rangle = \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = \exp[i\frac{\mu_p t}{\hbar} \begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix}]|\psi(0)\rangle$$

$$= \begin{pmatrix} \cos\frac{\mu Bt}{\hbar} + i\frac{B_z}{B}\sin\frac{\mu Bt}{\hbar} & \frac{iB_x + B_y}{B}\sin\frac{\mu Bt}{\hbar} \\ \frac{iB_x - B_y}{B}\sin\frac{\mu Bt}{\hbar} & \cos\frac{\mu Bt}{\hbar} - i\frac{B_z}{B}\sin\frac{\mu Bt}{\hbar} \end{pmatrix} |\psi(0)\rangle .$$

Si on s'arrange pour que B_x=B_y=0 (d'où B_z=B), on trouve que l'action de cette induction constante pendant un temps t est équivalente à une porte logique de déphasage, $\Delta\varphi = \frac{2\mu Bt}{\hbar}$:

$$\Phi(\Delta\varphi) = \begin{pmatrix} \exp[i\frac{\mu Bt}{\hbar}] & 0 \\ 0 & \exp[-i\frac{\mu Bt}{\hbar}] \end{pmatrix}.$$

Si on s'arrange pour que B_x=B_z et B_y=0 (d'où B_x=B_z=B/√2), on trouve que l'action de cette induction constante pendant un temps t tel que $\cos(\mu Bt/\hbar) = 0$ est équivalente à une porte logique de Hadamard. Toutefois cette procédure n'est jamais utilisée : d'une part imposer une induction constante agissant discontinûment est impossible à réaliser et d'autre part cela affecterait tous les noyaux sans distinction alors qu'on souhaite une action sélective sur un noyau particulier.

On résout le problème en superposant un champ constant, B_0, selon Oz et un champ, d'intensité B_1, tournant uniformément dans le plan Oxy. Nous connaissons le rôle joué par B_0

qui est de créer la différence énergétique entre les états de base. Celui joué par B_1 est de stimuler sélectivement les transitions, $|0\rangle \to |1\rangle$ et $|1\rangle \to |0\rangle$. Pour le voir, écrivons l'équation d'évolution,

$$i\hbar\partial_t \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = -\mu \begin{pmatrix} B_0 & B_1 e^{-i\omega t} \\ B_1 e^{i\omega t} & -B_0 \end{pmatrix} \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix}.$$

Elle est également soluble exactement sous la forme :

$$|\psi(t)\rangle = \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = \exp[-i\frac{\omega}{2}\sigma_z t]\exp\left[i\left((\frac{\omega}{2} + \frac{\mu B_0}{\hbar})\sigma_z + \frac{\mu B_1}{\hbar}\sigma_x \right) t \right] |\psi(0)\rangle$$

$$= \begin{pmatrix} \left(\cos\frac{\Omega t}{2} - i\frac{2\mu B_0 + \hbar\omega}{\hbar\Omega}\sin\frac{\Omega t}{2} \right) e^{-i\omega t/2} & \frac{2i\mu B_1}{\hbar\Omega}\sin\frac{\Omega t}{2\hbar} e^{-i\omega t/2} \\ \frac{2i\mu B_1}{\hbar\Omega}\sin\frac{\Omega t}{2} e^{i\omega t/2} & \left(\cos\frac{\Omega t}{2} - i\frac{2\mu B_0 + \hbar\omega}{\hbar\Omega}\sin\frac{\Omega t}{2} \right) e^{i\omega t/2} \end{pmatrix} |\psi(0)\rangle$$

où on a posé :

$$\Omega = \sqrt{4\mu^2(B_0^2 + B_1^2) + 4\mu\hbar\omega B_0 + (\hbar\omega)^2} = \sqrt{(2\mu B_0 + \hbar\omega)^2 + (2\mu B_1)^2}/\hbar .$$

Avec la technique du champ tournant, on contrôle sélectivement l'évolution en se plaçant à la résonance du noyau visé, résonance caractérisée par la relation,

$$\omega_{res} = -\frac{2\mu B_0}{\hbar} \qquad \Rightarrow \qquad |\psi(t)\rangle = \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = \begin{pmatrix} \cos\frac{\mu B_1 t}{\hbar} e^{i\mu B_0 t/\hbar} & i\sin\frac{\mu B_1 t}{\hbar} e^{i\mu B_0 t/\hbar} \\ i\sin\frac{\mu B_1 t}{\hbar} e^{-i\mu B_0 t/\hbar} & \cos\frac{\mu B_1 t}{\hbar} e^{-i\mu B_0 t/\hbar} \end{pmatrix} |\psi(0)\rangle .$$

On constate qu'à la résonance, on simule la porte de déphasage en un temps très court, $(\pi\hbar)/(\mu B_1)$, de l'ordre de la microseconde, la porte Not en un temps, $(\pi\hbar)/(2\mu B_1)$, et la porte de Hadamard (à deux portes de déphasages près, en fait, $\Phi_1 H \Phi_2$), en un temps $(\pi\hbar)/(4\mu B_1)$.

Hors résonance, le rapport $(\mu B_1)/(\hbar\Omega) \sim B_1/B_0$ peut être choisi suffisamment petit pour que la porte ne s'écarte pas de l'identité en un temps raisonnable en tous cas nettement plus court que le temps de calcul visé.

Evidemment puisque les portes de déphasages et de Hadamard sont universelles pour le qubit isolé, la même technique permet d'implémenter toutes les portes du type, $e^{\pm i\alpha\sigma_{x,y,z}}$, où $\sigma_{x,y,z}$ représente n'importe quelle matrice de Pauli.

La sélectivité qu'offre la résonance permet alors de construire une porte c-Not sur base des interactions spin-spin. On commence par observer que la transformation suivante inverse effectivement sélectivement un qubit « cible », t, en fonction de l'état d'un qubit de contrôle voisin, c :

$$cNot_c^t = e^{-i\pi/4}\exp[-i(\pi/4)\sigma_y^{(c)}]\exp[i(\pi/4)\sigma_x^{(c)}]\exp[i(\pi/4)\sigma_y^{(c)}]\exp[-i(\pi/4)\sigma_x^{(t)}]\exp[i(\pi/4)\sigma_y^{(t)}]$$
$$\exp[-i(\pi/4)\sigma_z^{(c)}\otimes\sigma_z^{(t)}]\exp[-i(\pi/4)\sigma_y^{(t)}]$$

Tous les opérateurs qui figurent dans cette expression ont une implémentation connue sauf un, $\exp[-i(\pi/4)\sigma_z^{(c)}\otimes\sigma_z^{(t)}]$, qui comme on pouvait s'y attendre, fait intervenir deux qubits simultanément. On peut espérer l'implémenter comme suit.

Les spins interagissent deux par deux de telle manière que chaque couple, (i, j), est caractérisé par une pulsation, ω_{ij}, parfaitement mesurable dont la valeur dépend évidemment de l'environnement. Ecrivons le hamiltonien et l'équation d'évolution correspondante dans le cas où n noyaux seraient présents :

$$H = \sum_j \hbar\omega_j Id^{(1)}\otimes\cdots\otimes\sigma_z^{(j)}\otimes\cdots\otimes Id^{(n)} + 2\sum_{j<k}\hbar\omega_{jk} Id^{(1)}\otimes\cdots\otimes\sigma_z^{(j)}\otimes\cdots\otimes\sigma_z^{(k)}\otimes\cdots\otimes Id^{(n)}$$
$$\Rightarrow \qquad i\hbar\partial_t|\psi\rangle = H|\psi\rangle$$

Dans cette équation les pulsations, ω, sont connues expérimentalement avec une grande précision. La solution s'écrit :

$$|\psi(t)\rangle =$$
$$\prod_j \exp[-i\omega_j Id^{(1)}\otimes\cdots\otimes\sigma_z^{(j)}\otimes\cdots\otimes Id^{(n)}t]\prod_{j<k}\exp[-2i\omega_{jk} Id^{(1)}\otimes\cdots\otimes\sigma_z^{(j)}\otimes\cdots\otimes\sigma_z^{(k)}\otimes\cdots\otimes Id^{(n)}t]|\psi(0)\rangle$$

dont la forme matricielle est trop barbare pour figurer ici. Il suffit de retenir qu'on peut solliciter le système par un champ tournant à la pulsation, ω_{jk}, voulue ce qui introduit le terme $\exp[-i(\pi/4)\sigma_z^{(c)}\otimes\sigma_z^{(t)}]$ requis par la porte c-Not.

Un lecteur attentif aura toutefois remarqué que la technique du champ résonant exige la présence d'un champ directeur constant orienté selon Oz qui a pour seule fonction de différencier les niveaux énergétiques et d'autoriser la résonance. Or ce champ sollicite tous les noyaux indistinctement y compris ceux que l'on ne veut pas voir évoluer à cet instant. Il convient de neutraliser cette évolution parasite et on y parvient en utilisant une astuce dont le principe repose sur la remarque suivante. Les évolutions quantiques étant unitaires, il doit toujours être possible de les invertir. Effectivement l'exemple suivant le montre : si un qubit évolue sous l'action de l'opérateur, $e^{+i\alpha\sigma_z}$, il suffit de le soumettre à deux transformations supplémentaires de type, σ_x, à savoir dans cet ordre, $\sigma_x e^{+i\alpha\sigma_z}\sigma_x = e^{-i\alpha\sigma_z}$, pour qu'il réintègre son état antérieur. On voit qu'à condition de tenir à jour sa comptabilité, il devient possible de programmer à la carte l'évolution des registres.

L'implémentation NMR remplit toutes les prescriptions du cahier des charges de l'ordinateur quantique sauf une : il ne semble pas possible d'étendre la dimension, n, du registre de travail au-delà de quelques dizaines de noyaux. Le nombre des fréquences de résonance augmente au moins quadratiquement (rien qu'en s'en tenant aux interactions spin-spin) en sorte que leur résolution devient problématique. On ne s'étonnera donc pas que si

l’implémentation NMR a été la première à enregistrer un modeste succès, celui-ci tarde à être amélioré.

Quel que soit l’avenir promis à l’ordinateur quantique, son principe offre une illustration au moins pédagogique des principes de la mécanique quantique et c’est à ce stade le seul bénéfice réel que l’on peut en tirer.

Algorithmes quantiques.

David Deutsch

Peter Shor

Simulation du calcul d'une fonction par réseau de portes quantiques.

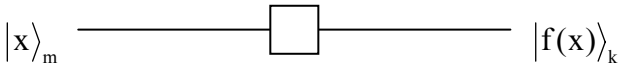
En agençant un nombre arbitraire de portes quantiques de toutes les manières possibles, on construit des réseaux qui transforment globalement n qubits d'entrée en n qubits de sortie. On peut naturellement concevoir la transformation résultante comme l'exercice du calcul d'une fonction, $f(x) : \{0,1\}^n \rightarrow \{0,1\}^n$. Toutefois c'est la question inverse et généralisée qui est la plus intéressante : peut-on toujours associer un réseau quantique à une fonction donnée, $f(x) : \{0,1\}^m \rightarrow \{0,1\}^k$? L'universalité au sens de Turing l'exige mais cela ne se fait pas sans précautions. L'ordinateur quantique ne considère que les portes unitaires donc invertibles ce qui exige que le nombres des bits d'entrée et de sortie coïncident (m=k) et encore cela ne suffit pas car même lorsque m=k, la majorité des portes restent non invertibles ainsi que le montre un simple argument de comptage.

Il existe 2^{k2^m} fonctions binaires, $\{0,1\}^m \rightarrow \{0,1\}^k$. Chacune de ces fonctions peut être vue comme une porte dont la table logique exprime les instances de la fonction. En particulier, il existe 2^{n2^n} fonctions binaires, $\{0,1\}^n \rightarrow \{0,1\}^n$, parmi lesquelles $2^n!$ seulement sont invertibles. Voici par exemple, dans le cas, n=2 :

une des 24 portes invertibles : $\begin{matrix} 0 & 0 \\ \rightarrow & \\ 0 & 0 \end{matrix} \quad \begin{matrix} 0 & 1 \\ \rightarrow & \\ 1 & 0 \end{matrix} \quad \begin{matrix} 1 & 1 \\ \rightarrow & \\ 0 & 1 \end{matrix} \quad \begin{matrix} 1 & 0 \\ \rightarrow & \\ 1 & 1 \end{matrix}$,

une des 232 (= 256-24) portes non invertibles : $\begin{matrix} 0 & 0 \\ \rightarrow & \\ 0 & 0 \end{matrix} \quad \begin{matrix} 0 & 1 \\ \rightarrow & \\ 1 & 0 \end{matrix} \quad \begin{matrix} 1 & 1 \\ \rightarrow & \\ 0 & 0 \end{matrix} \quad \begin{matrix} 1 & 0 \\ \rightarrow & \\ 1 & 1 \end{matrix}$.

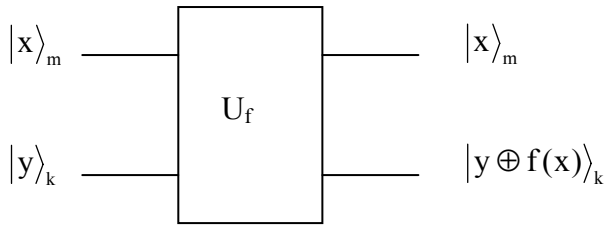
Il est, en général, inutile d'espérer construire un réseau quantique équivalent au calcul strict et rien de plus d'une fonction donnée, du type :



Si m≠k, c'est évident car un réseau quantique est toujours invertible et ce schéma ne l'est pas. Même lorsque m=k, nous savons qu'un calcul invertible exige qu'on ajoute aux données spécifiques du problème posé (les arguments de la fonction) un certain nombre de qubits de contrôle qui peuvent sans inconvénients être posés à zéro au début du calcul. A la fin du calcul, on récupère les résultats escomptés plus des qubits de déchet, inutiles en regard du problème posé mais indispensables pour garantir l'invertibilité du calcul. Le schéma précédent peut, par contre, toujours être remplacé par le suivant.

Quelle que soit la fonction classique, $f(x) : \{0,1\}^m \rightarrow \{0,1\}^k$, qui calcule k bits de sortie à partir de m bits d'entrée, il est possible de trouver une transformation unitaire (qui est d'ailleurs sa propre inverse), U_f, agissant sur les m qubits d'entrée plus k qubits supplémentaires, y, dits de contrôle tels qu'on retrouve intacts à la sortie les m qubits de

données flanqués de k qubits, y Xor f(x). En particulier, le calcul de f(x) s'obtient en posant les k qubits de y égaux à zéro.



On voit que le calcul quantique d'une fonction, $f(x) : \{0,1\}^m \rightarrow \{0,1\}^k$, ne se fait en toute certitude qu'à l'aide d'une porte de dimension, n=m+k, que l'on note :

$$U_f|x\rangle_m|y\rangle_k = |x\rangle_m|y \oplus f(x)\rangle_k .$$

Dans la base calculatoire, la représentation matricielle de U_f prend la forme d'une des $2^n!$ matrices de permutations. Illustrons ce qui vient d'être dit sur l'exemple, m=k=1.

Il existe 4 fonctions binaires, $f(x) : \{0,1\} \rightarrow \{0,1\}$, notées, f_0, f_1, f_2 et f_3. La table de leurs valeurs s'écrit :

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
0	0	0	1	1
1	0	1	0	1

La fonction, $f_2(x)$, par exemple, est telle que :

$$\begin{cases} B_{f_2}|0\rangle|y\rangle = |0\rangle|y \oplus 1\rangle \\ B_{f_2}|1\rangle|y\rangle = |1\rangle|y \oplus 0\rangle \end{cases}$$

et les autres suivent sur le même modèle. Les représentations matricielles des opérateurs, B_f, se notent, dans la base calculatoire habituelle :

$$B_{f_0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad B_{f_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad B_{f_2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad B_{f_3} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

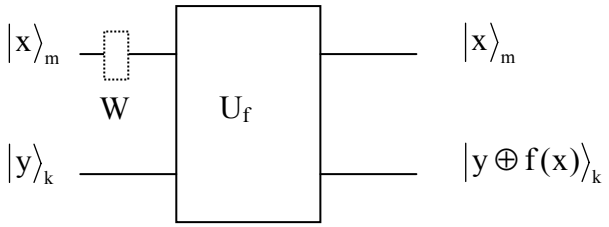
Calcul parallèle des valeurs d'une fonction.

La grande ambition de l'ordinateur quantique est d'être capable de traiter en parallèle un grand nombre, N, d'instances d'un problème donné. Dans l'exemple du calcul d'une fonction, f(x), il doit être capable d'évaluer en un seul passage l'application à tous les entiers binaires allant de 0 à 2^{m-1}. On y parvient comme suit.

On commence par préparer les données, $|x\rangle_m$, dans l'état de base particulier, $|000\cdots0\rangle$. Si on s'en tenait là, le réseau ne calculerait que f(0). Si on leur applique en sus l'opérateur de Walsh-Hadamard, $W = \bigotimes_{i=1}^{m} H$, elles entrent dans un état de superposition maximum :

$$W|000\cdots00\rangle = \frac{1}{\sqrt{2^m}} \sum_{i=0}^{2^m-1} |i\rangle,$$

qui peut être vu comme la superposition de tous les entiers binaires allant de 0 à 2^{m-1}. Le réseau de portes quantiques appliqué à ce nouvel état calculera, par linéarité, les 2^m instances de f(x), $\frac{1}{\sqrt{2^m}} \sum_{i=0}^{2^m-1} |i\rangle_m |f(i)\rangle$. Cette relation exprime le parallélisme quantique.



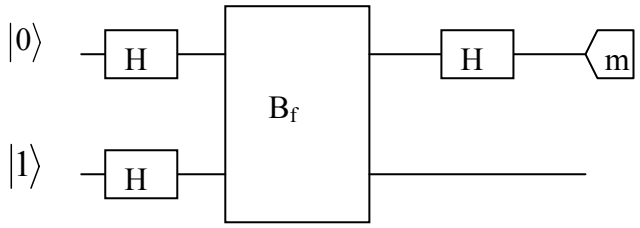
On pourrait se demander ce qu'on gagne concrètement du fait que pour prendre connaissance du résultat du calcul, une mesure effectuée sur les qubits de sortie est nécessaire qui ne révélera jamais qu'un seul des résultats calculés en parallèle et encore sans certitude a priori duquel il s'agira ! Cependant, on peut espérer montrer que soit ces probabilités d'occurrence ne sont pas égales et qu'elles favorisent à la longue certaines occurrences de solutions facilement vérifiables soit que quels que soient les tirages, certains invariants subsistent qui mènent à la solution cherchée.

On voit que la programmation quantique est un art très différent de son homologue classique. On ne connaît actuellement que fort peu d'algorithmes viables mais les recherches se poursuivent sur ce terrain neuf. Voici quelques exemples connus basés sur des principes d'action fort différents. Ils s'inspirent largement d'un exposé dû à John Watrous.

L'oracle de Deutsch.

Le problème apparenté suivant, encore dû à Deutsch, illustre la notion d'invariant. Un oracle est un système uniquement capable de répondre par oui ou part non à une question posée. Reconsidérons les 4 fonctions binaires, $f(x) : \{0,1\} \rightarrow \{0,1\}$, notées, f_0, f_1, f_2 et f_3. Deux, f_0 et f_3, sont dites constantes ($f(0)=f(1)$) et deux, f_1 et f_2, sont dites balancées ($f(0)\neq f(1)$). Imaginons que le réseau quantique qui calcule une de ces quatre fonctions est effectivement prisonnier d'une boîte noire dont le contenu est inaccessible sauf qu'on peut lui soumettre deux qubits d'entrée et mesurer les deux qubits de sortie, une opération qu'on appellera un « passage ». Combien de passages sont-ils nécessaires pour découvrir si la fonction cachée est constante ou balancée ?

Le même problème posé en informatique classique exige deux passages qui soumettent successivement l'argument x='0' puis x='1'. L'ordinateur quantique fait mieux : un seul passage suffit avec un coût minime d'un qubit additionnel de contrôle. Voici le design du réseau.



On peut suivre l'évolution du registre initial, $|0\rangle \otimes |1\rangle$, à mesure que les différentes portes sont franchies :

$$|0\rangle \otimes |1\rangle \xrightarrow{W} \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}|0\rangle \otimes (|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle \otimes (|0\rangle - |1\rangle)$$

$$\xrightarrow{B_f} \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{H} (-1)^{f(0)}|f(0) \oplus f(1)\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

On constate que quelle que soit la fonction cachée, $f_j(x)$ (j = 0, 1, 2, 3), la mesure du premier qubit donne '0' si f est constante et '1' si elle est balancée. Le deuxième qubit est inutile et il n'a pas besoin d'être mesuré. Cet algorithme fonctionne donc sur base de l'existence d'un invariant, $f(0) \oplus f(1)$, commun aux solutions cherchées.

On peut rechercher la représentation matricielle de l'opérateur, R, qui condense à lui seul la totalité des portes du réseau et vérifier qu'elle a bien le comportement annoncé. Voici l'exemple, R_2, associé à la fonction f_2 (attention à l'ordre !):

$$R_2 = (H_A \otimes Id_B) \cdot B_{f_2} \cdot (H_A \otimes H_B) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

$$R_2 \cdot (|0\rangle_A \otimes |1\rangle_B) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_A \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}_B$$

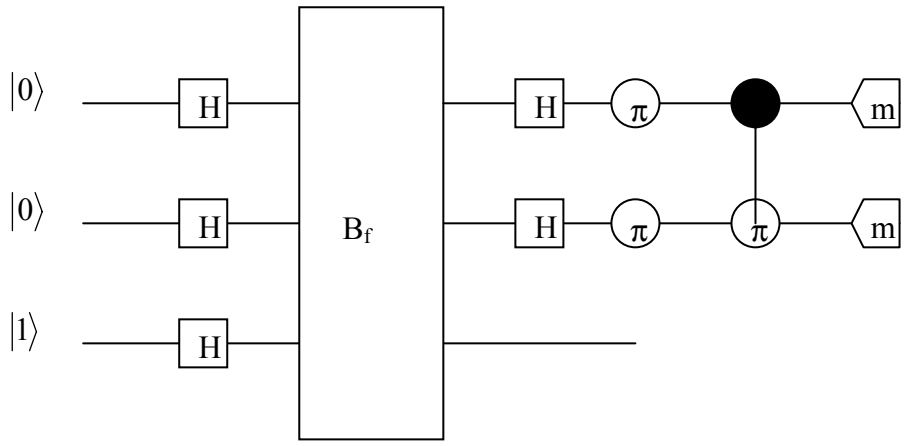
On voit que l'état final est factorisable et que la mesure du premier qubit le révèle obligatoirement dans l'état, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, signe que la fonction, f_2, est balancée.

Algorithme d'identification.

Il existe 16 fonctions binaires, $f(x) : \{0,1\}^2 \rightarrow \{0,1\}$, ce sont les fonctions booléennes de base. Nous allons enfermer une de ces fonctions dans une boîte noire mais pour ne pas compliquer l'exposé, nous convenons de nous restreindre à quatre d'entre elles, précisément :

pq	$f_8 = \text{Nor}(p,q)$	pq	$f_4 = p < q$	pq	$f_2 = p > q$	pq	$f_1 = \text{And}(p,q)$
00	1	00	0	00	0	00	0
01	0	01	1	01	0	01	0
10	0	10	0	10	1	10	0
11	0	11	0	11	0	11	1

Le problème posé consiste à découvrir en un seul passage laquelle de ces quatre fonctions la boîte noire calcule. Cet performance est manifestement hors de portée d'un ordinateur classique. Le réseau suivant répond à la question posée.



On peut le vérifier en suivant pas à pas l'évolution du registre ou en calculant la représentation matricielle équivalente, nécessairement 8x8, ou encore en recourant à la notation tensorielle. Les écritures sont trop lourdes pour être détaillées. Il s'avère que le troisième qubit est inutile et que la mesure des deux premiers livre la réponse cherchée selon le code :

$|00\rangle_{AB} \rightarrow f_8 \qquad |01\rangle_{AB} \rightarrow f_4 \qquad |10\rangle_{AB} \rightarrow f_2 \qquad |11\rangle_{AB} \rightarrow f_1 .$

Algorithme de recherche dans une base de données.

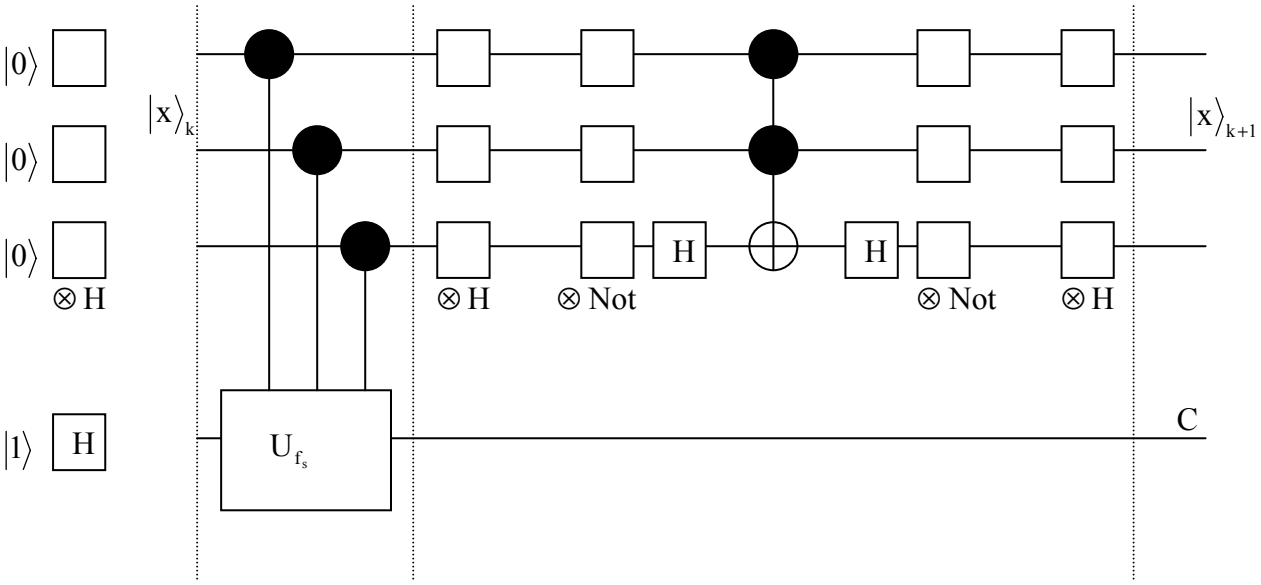
Les problèmes qui précèdent sont artificiels à plus d'un titre. D'une part, la question posée n'est pas particulièrement intéressante et d'autre part, personne ne passera jamais son temps à enfermer un système dans une boîte noire pour le plaisir de compliquer la situation. Le problème suivant est nettement plus réaliste. Rappelons qu'il existe 2^{2^n} fonctions, $f(x) : \{0,1\}^n \rightarrow \{0,1\}$ parmi lesquelles 2^n sont est nulles pour toutes les valeurs de ses variables sauf une, disons x_a. Le problème est précisément de trouver x_a tel que $f(x_a) = 1$. Vu que x_a est assimilable à une suite, s, de '0' et de '1', on voit que ce problème est apparenté à la recherche d'un abonné dans un annuaire classé dans l'ordre alphabétique quand on ne connaît que son numéro d'appel.

La fonction que nous avons en vue et son implémentation quantique se notent respectivement :

$$f_s(x) = \begin{cases} 0 & \text{si} \quad x \neq s \\ 1 & \text{si} \quad x = s \end{cases}$$

$$U_{f_s} |x\rangle |y\rangle = |x\rangle |y \oplus f_s(x)\rangle .$$

Le circuit suivant, imaginé par Grover résout par itération le problème posé :



Il se compose de n lignes (on n'en a dessiné que trois) qui encodent le vecteur d'état, $|x\rangle$, du système, à tout instant plus une ligne de contrôle, C. On prépare initialement le registre dans l'état de base, $|00\cdots0\rangle$, que l'on fait entrer dans l'état de superposition maximum grâce à n portes de Hadamard disposées en parallèle :

$$|x_0\rangle = \bigotimes_1^n H |00\cdots0\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle .$$

Quant au qubit de contrôle, C, on l'initialise dans l'état, $|1\rangle$, qu'une porte de Hadamard transforme immédiatement en : $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. En résumé, le système démarre dans l'état, $|x_0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Dans l'écriture du vecteur d'état, $|x_0\rangle$, les N états de base sont mis sur un pied d'égalité. La probabilité qu'une mesure du registre révèle, à ce stade, la valeur k cherchée ne vaut évidemment que $|\langle x_0|s\rangle|^2 = 1/N$, soit la valeur prédite par un tirage au sort honnête. C'est cette situation que le réseau conçu par Grover se propose d'améliorer. Ce réseau fonctionne itérativement, transformant à chaque passage le vecteur d'état, $|x_k\rangle$ $(k = 0,1,\cdots)$, en un nouveau vecteur d'état, $|x_{k+1}\rangle$, qui se rapproche de $|s\rangle$.

Il est commode de décomposer à tout instant le vecteur d'état selon la direction définie par $|s\rangle$ et la résultante des composantes orthogonales qui s'aligne sur $|u\rangle$. Au départ, on a :

$$|x_0\rangle = \sqrt{\frac{N-1}{N}}|u\rangle + \frac{1}{\sqrt{N}}|s\rangle = \cos(\theta/2)|u\rangle + \sin(\theta/2)|s\rangle$$

et on cherche λ_k et μ_k tels que l'on a encore à tout instant ultérieur,

$$|x_k\rangle = \lambda_k|u\rangle + \mu_k|s\rangle .$$

Le bloc itératif se compose de deux unités distinctes que la figure a séparé par un trait pointillé. Lors de la $k^{ième}$ itération, la première unité, qui est une porte U_f, a pour seul effet d'inverser le signe de la composante de $|x_k\rangle$ selon $|s\rangle$ (le qubit de contrôle n'est pas altéré) :

$$U_{f_s}|x_k\rangle \otimes \left|\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\rangle = \frac{1}{\sqrt{2}}|x_k\rangle \otimes \left(|0 \oplus f_s(x_k)\rangle - |1 \oplus f_s(x_k)\rangle\right) = (-1)^{f_s(x)}|x_k\rangle \otimes \left|\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\rangle$$
$$= \left(1 - 2|s\rangle\langle s|\right)|x_k\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (\lambda_k|u\rangle - \mu_k|s\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

La deuxième unité est d'apparence plus complexe bien que l'effet global soit simple : elle correspond à l'opérateur, $2|x_0\rangle\langle x_0| - \mathrm{Id}$, ce que l'on peut vérifier directement. Les calculs se résument comme suit :

$$|x_{k+1}\rangle = \lambda_{k+1}|u\rangle + \mu_{k+1}|s\rangle =$$
$$\left(2(\cos(\theta/2)|u\rangle + \sin(\theta/2)|s\rangle)(\cos(\theta/2)\langle u| + \sin(\theta/2)\langle s|) - \mathrm{Id}\right) \cdot (\lambda_k|u\rangle - \mu_k|s\rangle)$$

d'où le système récurrent satisfait par λ_k et μ_k :

$$\lambda_{k+1} = \lambda_k \cos\theta - \mu_k \sin\theta \qquad \mu_{k+1} = \mu_k \cos\theta + \lambda_k \sin\theta$$
$$\lambda_0 = \cos(\theta/2) \qquad \mu_0 = \sin(\theta/2)$$

On trouve que le système complet se trouve, après k itérations, dans l'état :

$$|x_k\rangle = \cos[(k+1/2)\theta]|u\rangle + \sin[(k+1/2)\theta]|s\rangle$$

et le qubit de contrôle n'est toujours pas altéré.

On constate que lorsque k est l'entier le plus proche de $(\pi/2\theta)$-0.5, soit encore de l'ordre de ,

$$k \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2},$$

$|x_k\rangle$ se confond quasiment avec $|s\rangle$. On voit qu'en gros, $\sqrt{N} = 2^{n/2}$ passages sont nécessaires, un gain appréciable par rapport à l'algorithme classique qui en exigerait 2^n. Par exemple, si $N=10^6$, $\theta = 2\arcsin(1/1000)$, et la probabilité qu'une mesure du registre, à l'étape k=785, fournisse l'ensemble des qubits encodés par $|s\rangle$ vaut $|\langle x_k|s\rangle|^2 = 0.9999999584$.

Factorisation des entiers longs : algorithme de Shor.

On sait que la confiance que l'on porte à la méthode désormais classique de cryptographie RSA repose sur deux conjectures jamais démontrées : 1) que la brisure du code RSA est synonyme de factorisation et 2) que cette factorisation n'est pas possible par des procédures classiques en un temps polynomial.

Aucune méthode classique de factorisation, de la plus naïve (Erathostène, en $O(\sqrt{N})$) à la plus évoluée (Pollard-Strassen, en $O\{\exp[(c\ell gN)^{1/3}(\ell g\ell gN)^{2/3}]\}$), ne résout le problème en un temps polynomial. Par contre, on sait, depuis 1994, qu'il existe un algorithme quantique, dû à Shor, qui est susceptible d'y parvenir à condition qu'un ordinateur quantique digne de ce nom voie jamais le jour. En 2001, le record est détenu par un groupe IBM qui a « réussi » à factoriser l'entier 15 mais ce n'est peut-être qu'un début. Il va donc de soi que cet algorithme ne menace pas immédiatement la cryptographie à clefs publiques à tel point que beaucoup pensent que la probabilité que l'ordinateur quantique devienne une réalité est bien moindre que celle d'une brisure du code RSA par une méthode différente de la factorisation. L'algorithme de Shor n'en vaut pas moins le détour.

La méthode de Shor déploie, en fait, une stratégie probabiliste qui lui assure de trouver un facteur premier de n'importe quel nombre composite avec une bonne probabilité. Toute tentative qui a échoué peut être recommencée jusqu'à ce qu'un facteur se dégage presque à coup sûr en un temps raisonnable. La méthode de Shor est un mélange de stratégies classique et quantique et il va de soi que les premières ne sont utilisées que lorsqu'elles sont effectives en un temps polynomial. Nous commençons par l'exposé du principe de la méthode. Soit à trouver un facteur premier de l'entier N.

1) Tester la primalité de N. On connaît depuis 2002 un algorithme (AKS) effectif en un temps polynomial. Si N est premier le problème est résolu : il n'existe pas de facteur premier autre que lui-même.

2) Sinon, choisir un entier, a (1<a<N), au hasard. Calculer, par l'algorithme d'Euclide, le pgcd de a et de N. S'il est différent de 1 on a, par chance, trouvé un facteur premier de N et le problème est résolu. Sinon on poursuit comme suit.

3) On construit la suite, $s_k = \mathrm{Mod}[a^k, N]$, inévitablement périodique de période, r, $s_{k+r} = s_k$.

4) Si r est impair ou si $\mathrm{Mod}[a^{r/2}, N] = \pm 1$, la procédure est en échec et il y a lieu de la reprendre au point 2 sur base d'une nouvelle valeur de a.

5) Sinon, deux facteurs de N sont respectivement : $\mathrm{pgcd}[a^{r/2} \pm 1, N]$.

Toutes ces étapes sont effectives en un temps polynomial sauf une : celle qui calcule la période, r, de la suite. Il est utile, à ce stade, de rappeler la méthode classique de détection de la période d'une suite. Elle est basée sur la transformée de Fourier discrète (TFD).

1) Extraction de la période d'une suite par transformée de Fourier discrète.

Soit une suite s_k, $(k = 0,1,\cdots,N-1)$, on définit ainsi sa TFD, $\tilde{s}_j$, $(j = 0,1,\cdots,N-1)$:

$$\tilde{s}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp[2i\pi \frac{jk}{N}] s_k \qquad \Leftrightarrow \qquad s_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp[-2i\pi \frac{jk}{N}] \tilde{s}_j$$

Lorsque la suite s_k est réelle, sa TFD ne l'est en général pas à l'exception de son premier élément qui vaut toujours la moyenne arithmétique de ses éléments. Les autres éléments de la TFD sont reliés par la relation : $\tilde{s}_j = \tilde{s}^*_{N-j}$ $(j = 1,\cdots,N-1)$. Cette propriété ne vaut plus si sa suite de départ est complexe.

Il existe un rapport étroit entre TFD et suites périodiques. On le met en évidence en considérant le prototype de la suite périodique, $s_k = \exp[2i\pi k\nu]$, de fréquence, $\nu \in]0,1[$, ou, si l'on préfère, de période, $T = 1/\nu$ (>1). La TFD de cette suite vaut exactement :

$$s_k = \exp[2i\pi k\nu] \qquad \Leftrightarrow \qquad \tilde{s}_j = \frac{1}{\sqrt{N}} \frac{\sin(N\pi\nu)}{\sin(\pi\nu + \pi j/N)} \exp\left[i\pi[(N-1)\nu - \frac{j}{N}] \right].$$

Il existe un cas idéal où la suite $\tilde{s}_j$ est nulle partout sauf en un point : il suffit que $N\nu$ soit entier, $N\nu = \ell$, ou, ce qui revient au même, que la période de la suite, T, divise sa longueur, N. Dans ce cas, la TFD est nulle partout sauf au point, j, calculé comme suit :

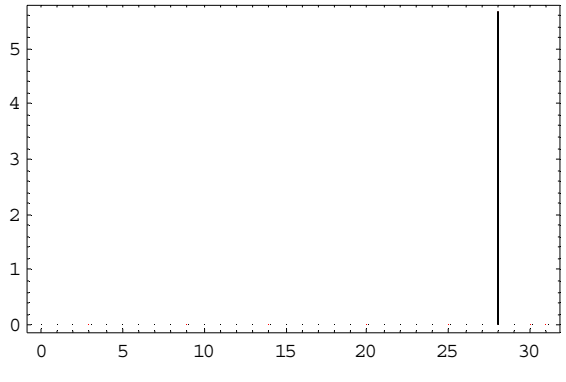
$$\sin(\pi\nu + \pi j/N) = 0 \qquad \Rightarrow \qquad j = N(1-\nu) \quad \text{(entier!)} \qquad \Rightarrow \qquad \tilde{s}_j = \sqrt{N} \neq 0.$$

Voici le détail de la TFD de la suite de fréquence 1/8, échantillonnée 32 fois, suivie de son graphe qui est réel dans ce cas particulier :

```
Simplify[Table[1/Sqrt[32] Sum[Exp[2 I π/8 k] Exp[2 I π k j/32], {k, 0, 31}], {j, 0, 31}]]
```

$$\{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4\sqrt{2}, 0, 0, 0\}$$

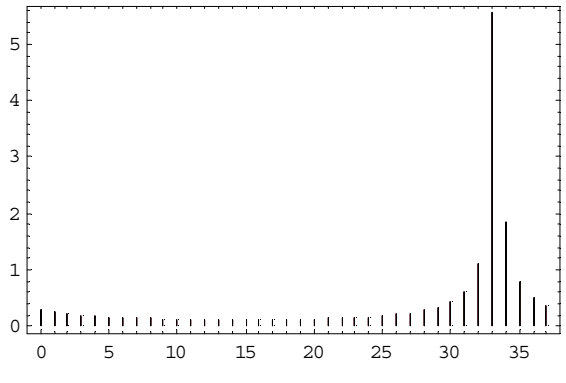
```
GeneralizedBarChart[Table[{j, Abs[Fourier[Table[Exp[2 I π/8 n], {n, 0, 31}]][[j + 1]], 0.0001}, {j, 0, 31}],
 PlotRange → All, Axes → False, Frame -> True]
```



($s_k = \exp[\frac{2i\pi}{8}k]$; ν = 1/8 d'où T = 8; N = 32)

Le graphe change lorsque N n'est plus un multiple de T : la suite, $\tilde{s}_j$, cesse d'être nulle presque partout. Toutefois, elle conserve un pic principal au voisinage de $N(1-\nu)$, qui a d'ailleurs cessé d'être un entier. Du fait que la TFD devient complexe on ne dessine que son module :

```
GeneralizedBarChart[Table[{j, Abs[Fourier[Table[Exp[2 I π/8 n], {n, 0, 37}]][[j + 1]], 0.0001}, {j, 0, 37}],
 PlotRange → All, Axes → False, Frame -> True]
```



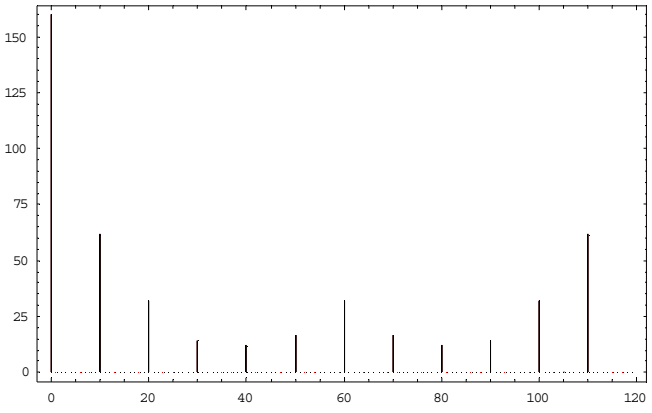
($s_k = \exp[\frac{2i\pi}{8}k]$; ν = 1/8 d'où T = 8; N = 38)

L'exemple considéré est très particulier. Une suite périodique quelconque possède une TFD plus compliquée. Considérons la suite, de période 12,

$s_k = \text{Mod}[2^k, 35] = \{1,2,4,8,16,32,29,23,11,22,9,18,1,2,4,8,\cdots\}$.

On constate, à nouveau, que si T divise N, la TFD continue d'être nulle sauf en quelques points isolés, onze dans l'exemple retenu en ignorant l'origine :

```
GeneralizedBarChart[Table[{j, Abs[Fourier[Table[Mod[2^n, 35], {n, 0, 119}]][[j + 1]], 0.0001}, {j, 0, 119}],
 PlotRange → All, Axes → False, Frame -> True]
```



($s_k = \mathrm{Mod}[2^k,35]$; T = 12 ; N = 120)

On explique cette démultiplication des pics en exprimant la suite comme combinaison linéaire de T exponentielles imaginaires du type, $\exp(2i\pi\ell k\nu_0)$ $(\ell = 0,1,\cdots,T-1)$. Cette opération est toujours possible à condition d'égaler la valeur de ν_0 à l'inverse de la période de la suite considérée. On trouve un nombre de termes égal à la période, T, soit, dans l'exemple, la décomposition suivante :

$$s_k = \mathrm{Mod}[2^k,35] = \sum_{\ell=0}^{T-1} c_\ell \exp[2i\pi\nu_0\ell k] = c_0 + c_1\exp[\frac{2i\pi}{12}k] + c_2\exp[\frac{2i\pi}{12}2k] + \cdots + c_{11}\exp[\frac{2i\pi}{12}11k]$$

Dans cette expression, le deuxième terme, $\ell = 1$, est toujours présent, c'est le fondamental de fréquence $\nu_0 = 1/T$. Les (T-2) termes qui suivent sont ses harmoniques, de fréquences, $\nu = \ell\nu_0 = \ell/T$ et il n'est pas exclu que certains harmoniques soient absents si la valeur du coefficient, c_j, qui lui est associée est nulle. Les c_j (j=0, …,11) se calculent simplement par inversion de la transformée de Fourier, soit, dans l'exemple :

```
c = Simplify[Table[1/12 Sum[Mod[2^j, 35] Exp[-2 i π/12 j k], {j, 0, 11}], {k, 0, 11}]]
```

$$\left\{\frac{175}{12}, -\frac{35}{24}\left((2-i)+\sqrt{3}\right), \frac{35}{12}(-1)^{1/3}, -\frac{7}{6}-\frac{7i}{12}, \frac{5}{24}\left(1+3i\sqrt{3}\right), \frac{35}{24}\left((-2+i)+\sqrt{3}\right),\right.$$
$$\left.-\frac{35}{12}, \frac{35}{24}\left((-2-i)+\sqrt{3}\right), \frac{5}{24}\left(1-3i\sqrt{3}\right), -\frac{7}{6}+\frac{7i}{12}, -\frac{35}{12}(-1)^{2/3}, -\frac{35}{24}(-1)^{1/6}\left((2-i)+\sqrt{3}\right)\right\}$$

En résumé, le terme constant est responsable de la contribution à l'origine et les autres termes contribuent chacun pour un pic dans la TFD, qu'on localise, en partant de la droite du graphe, aux positions, $j = N(1-\ell\nu_0)$ $(\ell = 1,2,\cdots,11)$. Les onze termes présentent, en effet, des fréquences, $\nu = \ell/T$, égales respectivement à : 1/12, 2/12, …, 11/12. On en conclut que, dans l'exemple choisi, la TFD sera non nulle aux abscisses, 0, 10, 20, 30, …, 110. C'est bien ce qu'on observe.

En pratique on procède plutôt en sens inverse : on cherche la période de la suite sur base du graphe de sa TFD. On inverse donc le raisonnement et on associe à chaque pic situé en j une fréquence, ν, valant :

$$\nu = \ell\nu_0 = \frac{\ell}{T} = 1 - \frac{j}{N}.$$

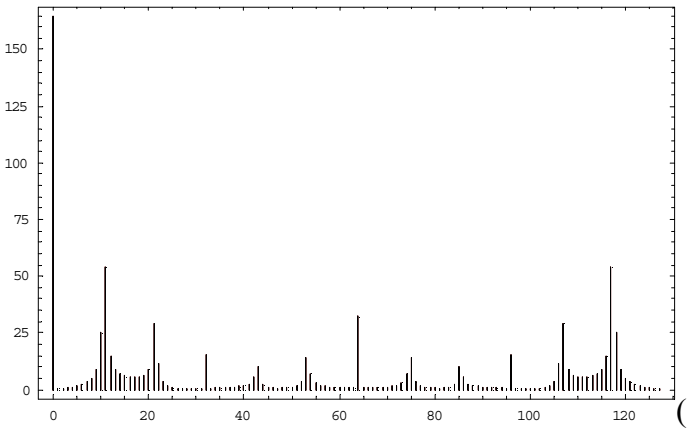
L'ensemble de ces fréquences forment la suite du fondamental et des harmoniques, soit dans l'exemple, {1/12, 2/12, 3/12, …, 11/12}, les pics étant lus de droite à gauche sur le graphe. La fréquence la plus basse, ν_0, correspond au dernier pic, obligatoirement toujours présent, et elle vaut l'inverse de la période cherchée, T=12, dans l'exemple.

Il résulte de ce qui précède que dans le cas particulier considéré où la longueur de la suite est un multiple de la période, la connaissance de la TFD d'une suite périodique renseigne immédiatement sur la valeur de sa période : il suffit de repérer la position, j, du dernier pic et d'appliquer la formule, T = N/(N-j). Si l'on applique la même formule en utilisant la valeur de j correspondant à un autre pic que le dernier, on trouve toujours un sous-multiple de la période.

Plusieurs problèmes subsistent cependant. Le premier est assez évident : on doit se fixer une longueur d'échantillonnage, N, pour la suite mais on ne connaît pas sa période, T, puisque précisément on la cherche. Sauf par chance extraordinaire, on se trouvera donc rarement dans le cas où T divise N et il convient de voir ce qu'on peut espérer de la méthode dans ce cas général.

Si T ne divise pas N, la TFD présente encore des pics principaux mais ils sont noyés dans un ensemble de pics ambiants plus petits d'où il résulte que le succès de l'analyse précédente n'est plus garanti. L'exemple suivant où la suite test est échantillonnée 128 fois le montre : le dernier pic principal se situe en j = 117. Or T = N/(N-j) = 128/(128-117) = 128/11 = 11.6364 ne livre certainement pas la période cherchée avec exactitude puisque ce n'est pas un entier mais elle n'en n'est pas très éloignée et une vérification de $s_T = s_0$ est après tout toujours possible !

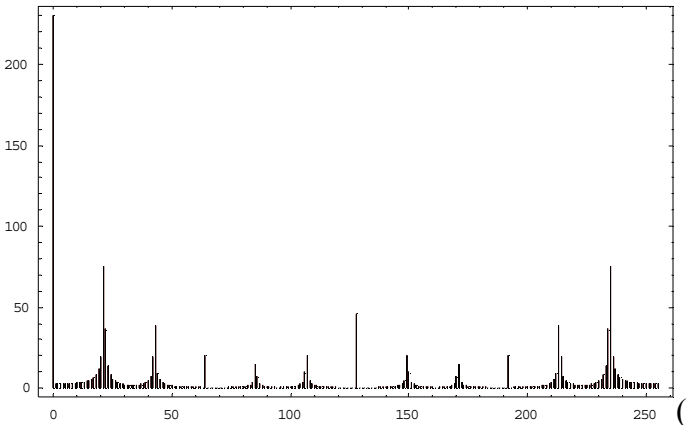
```
GeneralizedBarChart[Table[{j, Abs[Fourier[Table[Mod[2^n, 35], {n, 0, 127}]][[j + 1]], 0.00001}, {j, 0, 127}],
 PlotRange → All, Axes → False, Frame -> True]
```



(s_k = Mod[2^k,35] ; T = 12 ; N = 128)

On peut cependant remédier à cette situation de deux façons le cas échéant simultanément. La première consiste à allonger la suite. Voyons ce que devient l'exemple précédent si on double la longueur de l'échantillon, passant de N = 128 à 256 :

```
GeneralizedBarChart[Table[{j, Abs[Fourier[Table[Mod[2^n, 35], {n, 0, 255}]][[j + 1]], 0.0001}, {j, 0, 255}],
 PlotRange → All, Axes → False, Frame -> True]
```



($s_k = \text{Mod}[2^k,35]$; T = 12 ; N = 256)

On constate que les pics s'affinent et que la position du dernier d'entre eux, en j = 235, nous rapproche de la période cherchée : T = N/(N-j) = 256/(256-235) = 256/21 = 12.19. Si on localise par erreur le dernier pic principal en j = 234 ou 236, on trouvera une approximation de la période plus ou moins bonne, respectivement, 11.64 et 12.8. On voit que dans ce cas, la méthode cesse d'être sûre mais cela dit, il est toujours extrêmement facile de vérifier si on a bien, $s_T = s_0$, en essayant quelques valeurs qui encadrent l'approximation trouvée. Cette remarque peut paraître hors de propos dans la mesure où personne ne s'attend à commettre d'erreur dans le calcul d'une TFD. Elle ne l'est absolument pas dans l'optique d'une implémentation quantique de la TFD.

2) La transformée de Fourier quantique.

Une question préalable se pose toutefois : la procédure classique qui vient d'être décrite semble résoudre parfaitement le problème de l'extraction de la période d'une suite périodique. Dès lors pourquoi ne pas s'en contenter ? Le problème est que cette procédure n'est pas effective avec des ressources polynomiales. Le calcul complet d'une TFD sur un ordinateur classique requerrait un nombre d'opérations élémentaires de l'ordre du carré, N^2, du nombre que l'on veut factoriser (en fait, de l'ordre de $N\ell gN$ en recourant à l'algorithme rapide de Cooley & Tuckey) . A ce prix, autant recourir au crible d'Erathostène en $\sqrt{N}$!

Par contre l'ordinateur quantique fait beaucoup mieux car il est capable de calculer en parallèle tous les éléments d'une TFD. Considérons un registre, comprenant n qubits, qui évolue dans un espace de Hilbert à $N=2^n$ dimensions. Son vecteur d'état s'écrit :

$$|\psi\rangle = \sum_{j=0}^{2^n-1} c_j |j\rangle ,$$

dans la notation abrégée où les 2^n vecteurs de base, $|j\rangle$, sont ordonnés en suivant l'écriture binaire, de $|0\rangle = |00\cdots0\rangle$ à $|2^n-1\rangle = |11\cdots1\rangle$. Dans cette base, le vecteur d'état est

complètement caractérisé par la suite des amplitudes $\{c_j\}$, de longueur, 2^n. On définit la transformée de Fourier quantique du vecteur d'état (TFQ), $|\tilde{\psi}\rangle$, comme le vecteur d'état,

$$|\tilde{\psi}\rangle = \sum_{k=0}^{2^n-1} \tilde{c}_k |k\rangle,$$

où la suite $\{\tilde{c}_k\}$ est la TFD, $\tilde{c}_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \exp[2i\pi \frac{jk}{2^n}] c_j$, de la suite $\{c_j\}$.

Voici l'opérateur, $\hat{F}$, qui transforme $|\psi\rangle$ en $|\tilde{\psi}\rangle$, il est unitaire :

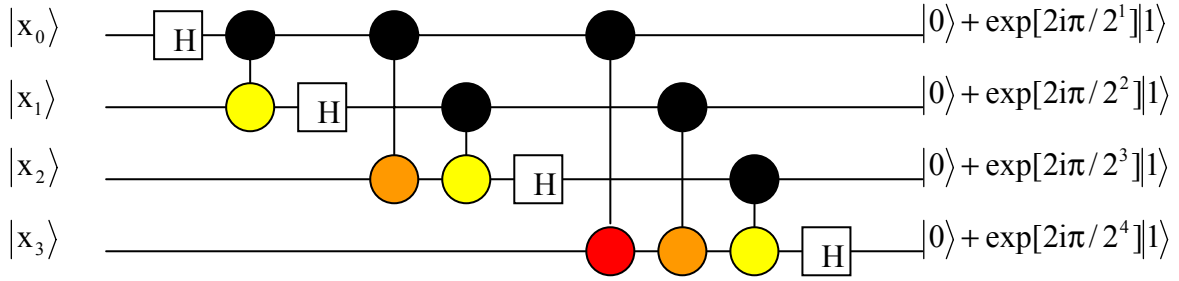
$$\hat{F} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} \exp[2i\pi \frac{jk}{2^n}] |k\rangle\langle j| \qquad \Rightarrow \qquad \hat{F}|\psi\rangle = |\tilde{\psi}\rangle.$$

Intéressons-nous au résultat de l'application de $\hat{F}$ à n'importe lequel des 2^n vecteurs de base, par exemple, $|\ell\rangle = |\ell_1 \ell_2 \cdots \ell_n\rangle$, on trouve que la TFQ se factorise comme suit :

$$\hat{F}|\ell\rangle =$$

$$|\tilde{\ell}\rangle = \frac{1}{\sqrt{2^n}} \left((|0\rangle + \exp[2i\pi 0.\overline{\ell_n}|1\rangle) \otimes (|0\rangle + \exp[2i\pi 0.\overline{\ell_{n-1}\ell_n}|1\rangle) \otimes \cdots \otimes (|0\rangle + \exp[2i\pi 0.\overline{\ell_1 \ell_2 \cdots \ell_n}|1\rangle) \right)$$

Cette factorisation est essentielle pour une conception récursive du circuit quantique capable d'implémenter la QFT quel que soit le nombre, n, de qubits qui composent le registre. Le réseau quantique correspondant utilise n portes de Hadamard et n(n-1)/2 portes induisant sous contrôle des déphasages du type, $p/2^j$ (j=0,1,2,…), (n=4 dans l'exemple représenté) :



Dans ce schéma la succession des portes s'écrit :

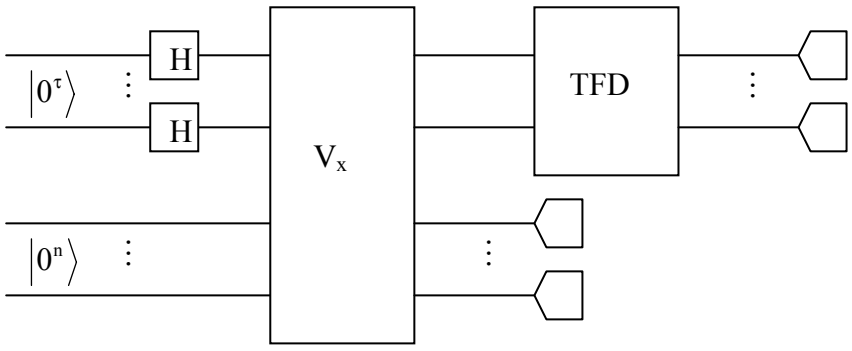
H_A $c\Phi(\pi)_{AB}$ H_B $c\Phi$ $(\pi/2)_{AC}$ $c\Phi$ $(\pi)_{BC}$ H_C $c\Phi$ $(\pi/4)_{AD}$ $c\Phi$ $(\pi/2)_{BD}$ $c\Phi$ $(\pi)_{CD}$ H_D.

L'idée sur laquelle repose l'algorithme de Shor est de se servir de la TFQ pour calculer en un seul passage la totalité de la TFD. Toutefois ce calcul massivement parallèle a un prix : celui de ne révéler qu'une valeur particulière de la TFD lors de la lecture du registre de sortie mais on verra que cela suffit à déterminer la période avec une bonne probabilité. Il est alors aisé de vérifier si $s_T = s_0$ et de recommencer la procédure si, par malchance, elle a échoué.

3) L'algorithme de Shor proprement dit.

Il existent plusieurs présentations plus ou moins économiques de l'algorithme mais nous avons préféré privilégier la clarté. Un exemple fera mieux comprendre comment l'algorithme fonctionne. Soit à factoriser le nombre N=21. On choisit un entier, a<N, premier avec N, soit a=2, par exemple. La suite, $\{2^k \text{ Mod } 21\}$ vaut : {1,2,4,8,16,11,1,2,4,8,16,11} et elle est de période paire, r = 6. Deux facteurs premiers de 21 sont donc : PGCD[$2^{r/2} \pm 1$,21] soit 3 et 7. Ce raisonnement a été facilité par le fait qu'une simple inspection de la suite a révélé la valeur de sa période mais cela cesse d'être possible lorsque N comporte quelques centaines de chiffres. Pour les besoins de l'exemple considéré nous allons faire comme si r était effectivement hors d'atteinte immédiate.

Nous optons pour la présentation suivante, empruntée à Lavor et al., pas forcément la plus économique mais sans doute la plus claire. Nous avons besoin de deux registres. Le premier comprend τ qubits, τ, tel que $N^2 \le 2^\tau < 2N^2$: τ = 9 est la plus petite valeur qui convient dans l'exemple considéré. Le deuxième registre comprend n qubits où, $n = \lceil \ell gN \rceil$, représente le nombre de bits nécessaires à l'encodage classique de N. Les deux registres sont initialisés dans les états de base, $|0^\tau\rangle$ et $|0^n\rangle$, et le système est décrit par le vecteur d'état, $|\psi_0\rangle = |0^\tau\rangle|0^n\rangle$, soit, dans l'exemple, $|\psi_0\rangle = |000000000\rangle|00000\rangle$, que l'on abrège comme d'habitude en $|\psi_0\rangle = |0\rangle|0\rangle$.



τ portes de Hadamard commencent par transformer cet état en,

$$|\psi_1\rangle = \frac{1}{2^{\tau/2}} \sum_{j=0}^{2^\tau - 1} |j\rangle|0\rangle = \frac{1}{\sqrt{512}} \sum_{j=0}^{511} |j\rangle|0\rangle .$$

Ensuite, l'opérateur V_x entre en action qui effectue l'opération unitaire :

$$V_x|j\rangle|k\rangle = |j\rangle|(k + x^j) \mod N\rangle .$$

A la sortie de cette porte, le système se trouve dans l'état suivant :

$$|\psi_2\rangle = V_x|\psi_1\rangle = \frac{1}{2^{\tau/2}}\sum_{j=0}^{2^\tau-1}|j\rangle|x^j \mod N\rangle.$$

Dans l'exemple, cela donne :

$$\begin{aligned}|\psi_2\rangle = \frac{1}{\sqrt{512}}[&(|0\rangle+|6\rangle+|12\rangle+\cdots+|510\rangle)|1\rangle+(|1\rangle+|7\rangle+|13\rangle+\cdots+|511\rangle)|2\rangle+\\ &(|2\rangle+|8\rangle+|14\rangle+\cdots+|506\rangle)|4\rangle+(|3\rangle+|9\rangle+|15\rangle+\cdots+|507\rangle)|8\rangle+\\ &(|4\rangle+|10\rangle+|16\rangle+\cdots+|508\rangle)|16\rangle+(|5\rangle+|11\rangle+|17\rangle+\cdots+|509\rangle)|11\rangle]\end{aligned}$$

On note que les deux premiers termes contiennent 86 termes alors que les quatre derniers en contiennent 85. L'état, $|\psi_2\rangle$, a ceci de remarquable que grâce au phénomène de superposition quantique, il contient la totalité de l'information que constituent les diverses puissances de x modulo N. Evidemment cette information n'est pas directement accessible puisque toute mesure a pour effet de ne révéler qu'une seule de ces puissances en détruisant les autres par projection.

Le moment est venu de mesurer l'état du second registre qui, dans l'exemple, ne peut livrer que l'un des six résultats suivants, avec des probabilités d'ailleurs égales : {1,2,4,8,16,11}. Supposons qu'il s'agisse du résultat '2'. Le système est projeté sur l'état propre renormalisé correspondant :

$$|\psi_3\rangle = \frac{1}{\sqrt{86}}((|1\rangle+|7\rangle+|13\rangle+\cdots+|511\rangle)|2\rangle) = \frac{1}{\sqrt{86}}\sum_{\ell=0}^{85}|6\ell+1\rangle|2\rangle.$$

Le premier registre est à présent projeté dans une superposition d'états dont les numéros d'ordre forment une suite périodique de période précisément égale à r. Peu importe le détail des termes de la suite, r est le renseignement vital qu'il nous faut extraire. On y parvient en appliquant une TFD portant sur τ qubits :

$$|\psi_4\rangle = \mathrm{TFD}|\psi_3\rangle = \frac{1}{\sqrt{2^\tau}}\sum_{j=0}^{2^\tau-1}\sum_{k=0}^{2^\tau-1}\exp[2i\pi\frac{jk}{2^\tau}]|k\rangle\langle j|\psi_3\rangle,$$

soit dans l'exemple :

$$|\psi_4\rangle = \mathrm{TFD}|\psi_3\rangle = \frac{1}{\sqrt{512}}\frac{1}{\sqrt{86}}\sum_{j=0}^{512}\left[\left(\sum_{\ell=0}^{85}\exp[2i\pi\frac{(6\ell+1)j}{512}\right)|j\rangle\right]|2\rangle.$$

Une mesure du premier registre, révèle la réponse, 'j', avec la probabilité,

$$p_j = \frac{1}{86\times512}\left|\sum_{\ell=0}^{85}\exp[2i\pi\frac{(6\ell+1)j}{512}\right|^2 = \frac{1}{86\times512}\frac{\sin^2(258\pi j/256)}{\sin^2(3\pi j/256)} \qquad (j=0,1,\cdots,511).$$

Dans cette dernière expression, une indétermination doit être levée en j=0 et 256, elle donne :

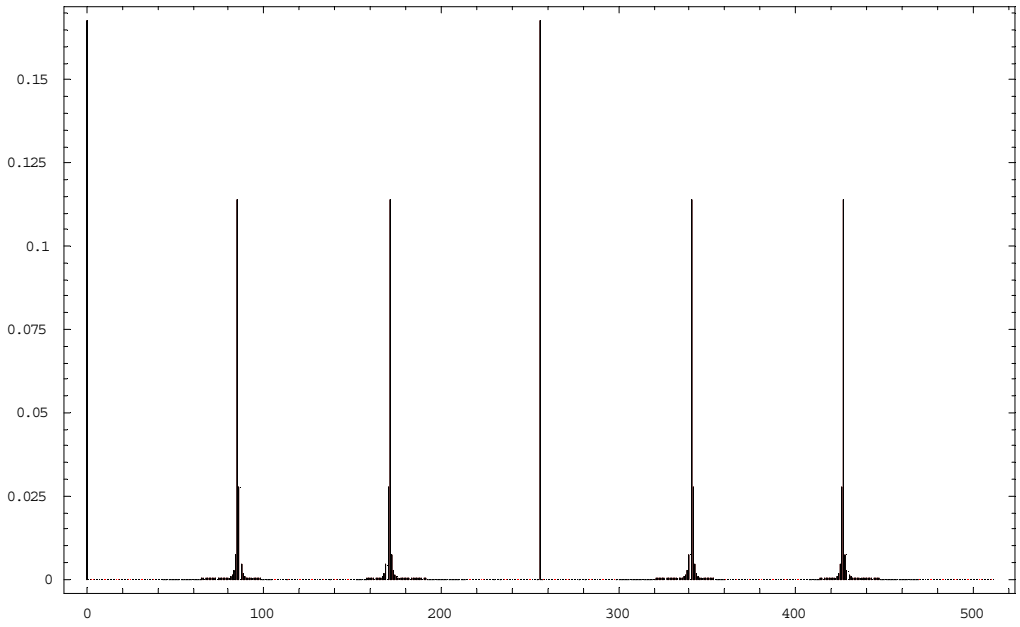
$$p_0 = p_{256} = \frac{86^2}{86 \times 512}.$$

On vérifie que l'on a bien que la somme des probabilités vaut 1 : $\sum_{j=0}^{511} p_j = 1$.

Le graphe de p_j est celui d'une fonction qui ne s'écarte notablement de zéro qu'en cinq endroits bien définis (l'origine étant ignorée), aux voisinages respectifs de :

j=85	j=171	j=256	j=341	j=427
(p_{85}=11.4)	(p_{171}=11.4)	(p_{256}=16.8)	(p_{341}=11.4)	(p_{427}=11.4)

Ces cinq valeurs de j représentent à elles seules 62.4% des cas possibles.



Partout ailleurs (sauf en l'origine qui est inexploitable et qui est « tirée au sort par la mesure dans 16.8% des cas), la probabilité tombe rapidement en-dessous de 0.001. Cela signifie que la mesure du premier registre révélera le plus fréquemment une des 5 valeurs intéressantes, 85, 171, 256, 341 ou 427. Il reste à appliquer à ces 5 valeurs de j, prises dans l'ordre inverse, la formule bien connue, (pour rappel, N=512) :

$$\nu = \frac{\text{N-j}}{\text{N}} \qquad \Rightarrow \qquad \nu_0 = \frac{85}{512}; \nu_1 = \frac{171}{512}; \nu_2 = \frac{256}{512}; \nu_3 = \frac{341}{512}; \nu_4 = \frac{427}{512};$$

La période cherchée vaut l'inverse de la fréquence la plus basse, $1/\nu_0 = 512/85 = 6.023$, soit plus que probablement la valeur cherchée, T = r = 6.

En pratique l'extraction de la période ou d'un de ses sous-multiples si la mesure a révélé autre chose que le dernier pic, se fait sur base du développement en fractions continues de la valeur trouvée pour la fréquence. Le développement de ν_4 donne :

$$\nu_4 = \frac{427}{512} = \frac{k}{r} = \cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{42+\cfrac{1}{2}}}}$$

soit la suite des approximants, 1/1, **5/6**, 211/253,427/512.

On trouve la période cherchée, r, comme le dénominateur de l'approximant le plus précis dont le dénominateur n'excède toutefois pas N (en effet, r<21). On trouve le période vaut très probablement 6.

Le même calcul effectué sur ν_1 donne :

$$\nu_1 = \frac{171}{512} = \frac{k}{r} = \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{170}}}$$

soit la suite des approximants, 1/2, **1/3**, 171/512. Le meilleur dénominateur est 3 qui n'est pas la période mais un de ses sous-multiples. Cette technique d'extraction est tout à fait remarquable car on montre qu'elle continue de fonctionner même si l'on s'écarte modérément du pic principal. Par exemple, il suffit que la mesure révèle une valeur de j comprise entre 163 et 178 pour que le développement en fraction continue fournisse toujours 3 comme facteur probable de la période ainsi qu'en attestent les listes des approximants pour des valeurs de j allant de 162 à 179 :

```
Table[Convergents[ContinuedFraction[j/512]],{j,162,179}]
```

$$\left\{\left\{0, \frac{1}{3}, \frac{6}{19}, \frac{25}{79}, \frac{81}{256}\right\}, \left\{0, \frac{1}{3}, \frac{7}{22}, \frac{78}{245}, \frac{163}{512}\right\}, \left\{0, \frac{1}{3}, \frac{8}{25}, \frac{41}{128}\right\},\right.$$
$$\left\{0, \frac{1}{3}, \frac{9}{28}, \frac{10}{31}, \frac{29}{90}, \frac{68}{211}, \frac{165}{512}\right\}, \left\{0, \frac{1}{3}, \frac{11}{34}, \frac{12}{37}, \frac{83}{256}\right\}, \left\{0, \frac{1}{3}, \frac{15}{46}, \frac{76}{233}, \frac{167}{512}\right\},$$
$$\left\{0, \frac{1}{3}, \frac{21}{64}\right\}, \left\{0, \frac{1}{3}, \frac{33}{100}, \frac{34}{103}, \frac{169}{512}\right\}, \left\{0, \frac{1}{3}, \frac{85}{256}\right\}, \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{171}{512}\right\}, \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{43}{128}\right\},$$
$$\left\{0, \frac{1}{2}, \frac{1}{3}, \frac{24}{71}, \frac{25}{74}, \frac{74}{219}, \frac{173}{512}\right\}, \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{17}{50}, \frac{35}{103}, \frac{87}{256}\right\}, \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{13}{38}, \frac{27}{79}, \frac{175}{512}\right\},$$
$$\left.\left\{0, \frac{1}{2}, \frac{1}{3}, \frac{11}{32}\right\}, \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{9}{26}, \frac{28}{81}, \frac{177}{512}\right\}, \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{8}{23}, \frac{89}{256}\right\}, \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{7}{20}, \frac{43}{123}, \frac{179}{512}\right\}\right\}$$

La procédure échoue en j=162 ou 179 car l'algorithme suggérerait une période erronée valant 19 ou 20. Toutefois ces événements malencontreux sont extrêmement peu probables, p_{162} = 0.000126 ou p_{179} = 0.0002245. En recommençant toute la procédure un nombre suffisant de fois, on fait apparaître les facteurs probables de r. Le ppcm de ces facteurs permet de remonter à r avec une probabilité proche de 1. L'incertitude qui subsiste est facile à dissiper : il suffit de vérifier que la période convient et que l'on a bien $s_T = s_0$.

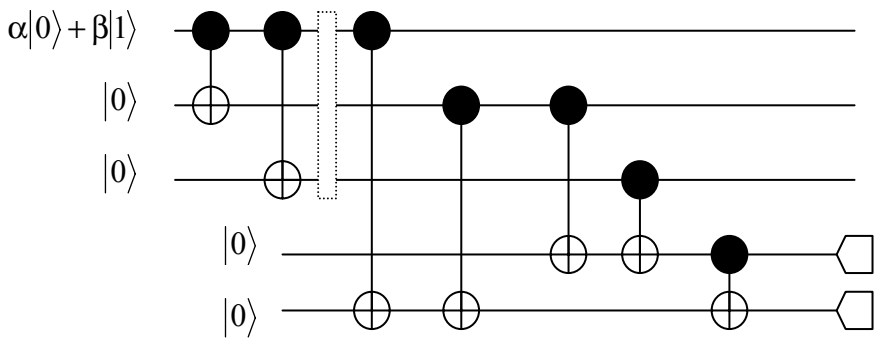
Corrections d'erreurs.

Les énormes difficultés qu'il y a à préserver tout registre quantique des influences décohérentes du milieu environnant représentent l'entrave majeure à la réalisation d'un prototype d'ordinateur quantique. Le problème est si aigu que la solution n'est nullement écartée de l'adoption d'un protocole massif de corrections d'erreurs. En d'autres termes, plutôt que d'essayer de maintenir à tout prix la cohérence des registres, on envisage de mettre en place, à tous les stades du calcul, des transformation qui passent les registres en revue et les restaurent automatiquement s'ils sont corrompus. Bien entendu de telles procédures consomment des ressources de qubits supplémentaires mais on estime généralement que ce coût reste modéré par rapport à ce que représenterait la mise en place d'une cohérence parfaite.

La correction automatique d'erreurs se fait sur le même principe qu'en théorie classique de l'information en recourant à des (qu)bits supplémentaires qui créent la redondance nécessaire. Toutefois le problème se complique en théorie quantique du fait que les vecteurs d'états ne sont pas forcément dans l'état logique '0' ou '1' mais qu'ils peuvent être en superposition des deux. Il faut, en particulier, pouvoir corriger des erreurs de déphasages sans perdre de vue que le clonage pur et simple est impossible. Nous ne faisons qu'effleurer ce sujet vaste et complexe.

Rappelons le principe du code correcteur classique le plus élémentaire qui soit : il est question d'envoyer un bit au travers d'un canal de transmission bruité de telle manière que la probabilité qu'il soit malencontreusement inversé soit égale à p. Le correspondant ne reçoit le bit correct qu'avec la probabilité (1-p). Une stratégie élémentaire consiste à envoyer trois copies du même bit que le receveur décodera à la majorité simple. Si $p<1/2$, on constate que la probabilité de décodage erroné tombe de p à $3p^2-2p^3$. Ce n'est pas parfait mais il y a un progrès. Si l'on veut faire beaucoup mieux, il y a lieu de mettre des procédures plus compliquées.

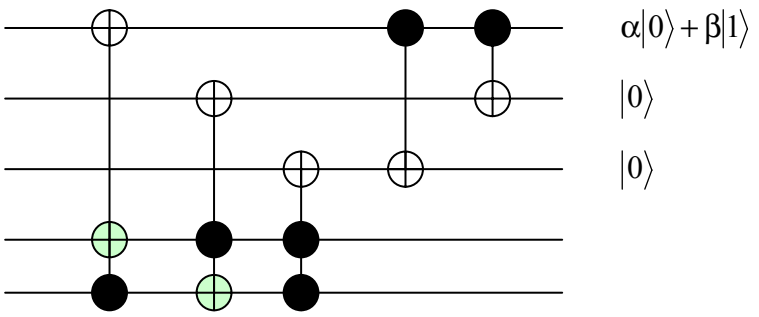
Cette procédure n'est pas applicable telle qu'elle à la transmission d'un qubit lorsque celui-ci est en état de superposition inconnu, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. D'une part, le théorème de non-clonage interdit de réaliser les deux copies nécessaires de $|\psi\rangle$ et de plus, mesurer les trois qubits envoyés afin de décoder à la majorité n'aurait aucun sens puisque la mesure a pour effet de détruire l'état mesuré. En fait, dans le montage qui suit, quatre qubits supplémentaires, préparés dans l'état de base, $|0\rangle$, sont utilisés à l'émission :



Supposons qu'on veuille protéger un qubit inconnu, $\alpha|0\rangle+\beta|1\rangle$, contre l'inversion accidentelle, '0' $\leftrightarrow$ '1'. On commence par utiliser deux portes c-Not afin de l'encoder dans un registre à trois qubits, sous la forme, $|\psi_0\rangle=\alpha|000\rangle+\beta|111\rangle$. Rappelons que sur ce genre de figure, l'axe horizontal, lu de gauche à droite, représente la ligne du temps. Le rectangle pointillé représente une zone temporelle où une corruption d'inversion menace de se produire avec une probabilité que nous n'avons pas besoin de connaître. A la sortie de cette zone, le registre se trouvera dans l'un des quatre états suivants dont trois sont altérés :

$$\mathrm{Id}\otimes\mathrm{Id}\otimes\mathrm{Id}|\psi_0\rangle \qquad \mathrm{Not}\otimes\mathrm{Id}\otimes\mathrm{Id}|\psi_0\rangle \qquad \mathrm{Id}\otimes\mathrm{Not}\otimes\mathrm{Id}|\psi_0\rangle \qquad \mathrm{Id}\otimes\mathrm{Id}\otimes\mathrm{Not}|\psi_0\rangle.$$

Plutôt que d'essayer d'empêcher cette corruption, on préfère l'accepter mais on ajoute un circuit, composé de cinq portes c-Not correctement agencées, qui ont pour effet de restaurer le registre dans les quatre cas de figure. Avec un peu de patience on peut se convaincre que le circuit fonctionne comme suit : les trois qubits parviennent à Bob dans l'état éventuellement altéré, $|\psi_0\rangle=\alpha|000\rangle+\beta|111\rangle$. Les deux derniers qubits ne sont que des auxiliaires qui peuvent être mesurés par Bob. Celui-ci trouvera, dans tous les cas, le numéro binaire du qubit altéré (00 = pas d'altération, 01 = altération du premier qubit, 10 = altération du deuxième qubit, 11 = altération du troisième qubit). Selon la valeur du syndrome trouvé, il reste à Bob à réappliquer une porte Not au qubit altéré puis à inverser la manœuvre réalisée par Alice afin d'extraire $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ de $|\psi_0\rangle=\alpha|000\rangle+\beta|111\rangle$. Ces deux manœuvres peuvent être faites automatiquement sans même qu'une mesure soit effectuée. Il suffit que Bob utilise le circuit de réception suivant, où les trois premières portes c-Not corrigent l'erreur (le qubit de contrôle gris est inversé : le contrôle ne commande l'instruction Not que s'il est mis à '0') et les deux dernières portes extraient $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ de $|\psi_0\rangle=\alpha|000\rangle+\beta|111\rangle$:



Au bilan ce réseau répare l'éventuelle inversion isolée d'un qubit. Hélas l'histoire ne s'arrête pas là. L'inversion d'un qubit n'est qu'un avatar parmi d'autres que peut subir le qubit. L'altération la plus générale revêt nécessairement la forme suivante

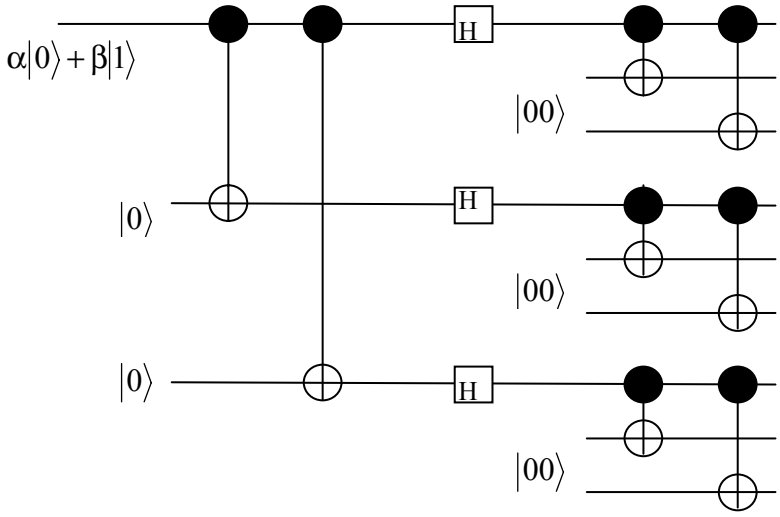
$$|\psi_{alt}\rangle=(e_1\mathrm{Id}+e_2\sigma_x+e_3\sigma_y+e_4\sigma_z)|\psi\rangle,$$

où les coefficients, e_i, peuvent être complexes. Dans l'exemple précédent, l'inversion correspondait au cas particulier, Not = σ_x. $\sigma_z=\Phi(\pi)$ correspondrait à une inversion de phase. Or les réseaux qui précèdent sont impuissants à corriger ne serait-ce qu'une inversion de phase et ce qu'il nous faut c'est une procédure effective dans tous les cas.

Il n'est pas question d'étudier ici les détails de cette procédure générale. On peut se faire une idée des complications auxquelles il faut s'attendre en contemplant la solution que Shor a trouvée pour régler le cas pas encore général où on veut corriger à la fois une inversion de bit et de phase. Une solution à ce problème nécessite un encodage préalable du qubit à protéger, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, sous la forme d'un registre à 9 qubits :

$$|\psi_0\rangle = \alpha\frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} + \beta\frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

que l'on obtient en utilisant le réseau suivant :



Ce réseau n'est que la première étape, celle de l'encodage redondant. Il faut encore installer le circuit correcteur puis celui de désencodage qui extrait $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ de $|\psi_0\rangle$ dans tous les cas d'une inversion de bit ou de phase. On voit que le réseau commence à prendre de l'ampleur exigeant un nombre croissant de qubits auxiliaires. La situation s'aggraverait évidemment dans le cas d'une altération supplémentaire par σ_y ou dans le cas d'une altération de plusieurs qubits. Toutefois, malgré le caractère inquiétant de ces complications, on peut montrer que le nombre de portes nécessaires ne croît que polynomialement ce qui permet de ne pas disqualifier la méthode.

Bob, Alice et les autres.

Les applications qui suivent impliquent, de près ou de loin, une communication à distance selon un canal de transmission. On ne s'étonnera pas que le photon soit considéré, dans ces cas, comme le système idéal d'encodage des qubits.

Nous poserons systématiquement le problème de la manière suivante : deux correspondants, traditionnellement appelés, Alice et Bob, désirent échanger de l'information. Alice est par convention l'émettrice et Bob le receveur. Nous admettrons que le canal de

transmission n'est pas bruité ou, si ce n'est pas le cas, que toutes les précautions ont été prises en termes de protocoles de corrections d'erreurs.

La théorie prévoit dans certains cas qui privilégient la confidentialité l'intervention d'un troisième larron, baptisé Eve (!), qui a pour mission d'espionner passivement les canaux de transmission. L'espion actif, qui intercepte et falsifie la transmission dans un but malveillant se nomme habituellement Oscar : ses interventions sont nettement plus redoutables que celles d'Eve et elles nécessitent la mise en œuvre de protocoles évolués. Nettement plus fréquentable est Walter, qui est chargé de certifier le bon déroulement des transactions effectuées par Alice et Bob, par exemple, du type commerciales à distance.

Les applications qui impliquent une communication à distance sont nombreuses et nous n'en retiendrons que trois : la cryptographie quantique, le codage dense et la téléportation. Elles représentent les espoirs les plus sensés de l'informatique quantique de l'an 2000. Le fait est que la communication n'implique que la maîtrise au compte-gouttes de photons isolés, faciles à préparer et à mesurer. La technologie sous-jacente est nettement moins intimidante que celle qui déboucherait sur un ordinateur quantique.

Distribution quantique des clefs.

Nous avons vu par ailleurs qu'aucune méthode cryptographique classique n'est sûre. Toutes les méthodes imaginables aussi tordues soient-elles contiennent l'information cachée et sont de ce fait exposées à être dévoilées. La seule perspective qui s'offre aux encrypteurs est de compliquer la tâche d'espions éventuels afin d'allonger tellement démesurément le temps de décodage qu'il en devient prohibitif. La méthode RSA, dite à clefs publiques, ne voit sa sécurité garantie que par la lenteur de l'ordinateur classique et par l'acte de foi que le problème de la factorisation des entiers longs est incontournable et non polynomial.

Il nous faut quand même tempérer l'affirmation qu'aucune méthode cryptographique classique n'est sûre : il existe bien une méthode classique fiable à 100% mais elle exige d'utiliser une clef de (dé)chiffrement aléatoire aussi longue que le texte à encrypter et de ne l'utiliser qu'une seule fois ! Si cette possibilité paraît ridicule, c'est évidemment que cette clef doit être échangée entre les correspondants par un canal sûr et que dans ces conditions on a aussi vite fait d'utiliser ce canal sûr pour échanger le message lui-même ! Elle a pourtant été mise à l'essai en utilisant des porteurs de confiance, le texte crypté n'étant échangé que lorsqu'il était certain que la clef était parvenue, sans encombres, à destination. Ces essais n'ont pas survécu aux coûts de la manœuvre.

La théorie quantique de l'information rend cependant une nouvelle jeunesse à cette méthode. Bennett et Brassard ont en effet mis au point un protocole peu coûteux qui assure une transmission inviolable des clefs. Plus exactement les deux correspondants, Alice et Bob, ont la possibilité d'échanger une clef en ayant la certitude que si elle est interceptée par un espion, Eve, ils en seront informés. Ce n'est que lorsqu'ils ont la certitude de n'avoir pas été espionnés qu'il peuvent échanger en toute quiétude le message crypté sur un canal qui n'a même pas besoin d'être sûr.

La méthode exige deux canaux de communication entre Alice et Bob. Le premier canal achemine au compte-gouttes des photons, dans divers états de polarisation linéaire, le

long d'une fibre optique par exemple. Le second est une voie de communication classique dont nous préciserons l'usage ultérieurement. Voyons d'abord comment les choses se passent dans le cas idéal où aucun espion n'est présent. Alice envoie à Bob des photons qu'elle prépare individuellement et aléatoirement dans un des quatre états de polarisation linéaire, x, y ou à 45° dans les deux sens, soit schématiquement, {-, | }∈mode(+) et { /, \}∈mode(X). Alice associe, à sa convenance, les valeurs '0' et '1' à chaque état complémentaire et elle ne change jamais de convention. Par exemple, elle envoie les photons suivants, en respectant l'encodage, (- ou \ →'0' et | ou /→'1') :

- | / - \ / \ \ \ \ / - / / - - \ \ | / | - -	(suite aléatoire sur l'alphabet, - | / \)
0 1 1 0 0 1 0 0 0 0 1 0 1 1 0 0 0 0 1 1 1 0 0	(sa traduction en '0' et en '1')
+ ++ XX XX ++ + ++ X + + +X ++ X+ X X	(bases choisies aléatoirement par Bob)
- || / \ / \ -| - - - / | - - \ - | / | \ /	(résultats des mesures faites par Bob)
0 1 1 1 0 1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 1 1 0	(leur traduction en '0' et '1')

Bob est parfaitement au courant de l'orientation des axes x et y (les deux correspondants peuvent se mettre d'accord lors d'un échange préparatoire d'information banale) ainsi que de l'encodage des bits adopté par Alice (en l'occurrence, - et \ pour encoder '0' et | et / pour encoder '1') mais il ignore totalement la suite (aléatoire) des orientations des polariseurs choisies par Alice lors de l'encodage. Il procède néanmoins à un décodage en variant lui aussi aléatoirement l'orientation de ses propres polariseurs selon les bases + ou X. Il va de soi qu'il se trompe d'orientation en moyenne une fois sur deux (les choix erronés ont été soulignés dans l'exemple cité).

Lorsque cette opération est terminée, les deux correspondants prennent contact par une voie téléphonique quelconque qui n'a pas besoin d'être sécurisée et dressent la liste des numéros d'ordre des photons pour lesquels ils ont fortuitement adopté la même orientation des polariseurs. Les bits restants, en gros la moitié des bits transmis, constituent une clef secrète potentiellement valable. Dans l'exemple, la clef qui subsisterait s'écrirait : 0 1 0 1 0 0 1 0 0 0 1 1 1. Toutefois il ne serait pas raisonnable de l'utiliser telle quelle. Les correspondants doivent, en effet, absolument contrôler l'absence d'intervention d'Eve. Pour ce faire, il existe une méthode élégante qui fait le prix de la cryptographie quantique : il suffit que Bob et Alice échangent par téléphone une partie de la clef obtenue de part et d'autre, par exemple les bits impairs ou multiples de 4 et qu'ils les jettent à la poubelle par mesure de précaution. Si ce sondage révèle une coïncidence parfaite c'est que le canal de transmission est resté inviolé. Par contre que faut-il penser du cas où Eve a espionné le canal de transmission ?

Posons-nous la question autrement : de quels moyens Eve dispose-t-elle pour espionner ce canal ? Au pis, elle pourrait : 1) être informée des orientations utilisées, + et X, 2) intercepter les photons envoyés par Alice et procéder à leur mesure enfin, 3) renvoyer les photons vers Bob dans l'état où sa mesure les a projeté. Par contre, elle ne connaît aucune des suites aléatoires des orientations des polariseurs choisies par Alice et par Bob. Elle en est donc réduite à se choisir sa propre suite mais cela va altérer gravement l'état des photons que Bob va recevoir. Alice et Bob vont immanquablement s'en apercevoir lors de leur sondage.

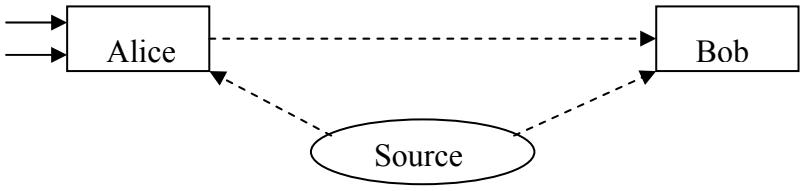
En effet, Eve va se tromper dans l'orientation des polariseurs en moyenne une fois sur deux. Les photons qu'elle va retransmettre à Bob vont provoquer un taux d'erreur sur la clef de 25% ce dont Alice et Bob vont inévitablement se rendre compte lors de la phase de contrôle. S'il s'avère que la transmission a été interceptée, Alice et Bob interrompent de commun accord leur échange sinon Alice envoie le message crypté selon la clef définie.

Il existe des stratégies d'espionnage plus subtiles où Eve peut intriquer les photons interceptés en provenance d'Alice avec des photons ancillaires de sa fabrication avant de les renvoyer vers Bob dans leur forme altérée. Quelle que soit la méthode retenue par Eve, il lui est impossible de faire descendre le taux d'erreurs en-dessous de 15%, une valeur largement suffisante pour être détectée lors du sondage de contrôle. Entre les cas extrêmes où le taux d'erreur est nul (où l'échange du message codé peut se faire en toute sécurité) et celui où il est supérieur à 15% (où l'échange doit être interrompu), les choses se compliquent du fait qu'il est impossible de savoir si les erreurs constatées sont dues à un bruit dans le canal de transmission ou à un espion qui tenterait de se camoufler en n'interceptant qu'une partie des photons. Dans de tels cas il faut recourir à des techniques plus sophistiquées qui préservent la confidentialité. Ces techniques débordent d'un exposé élémentaire.

Il existe une multitude d'attaques variées possibles et de réponses adaptées qu'il est impossible de détailler dans un exposé élémentaire. Cela étant, la distribution quantique des clefs n'est plus une fiction : les premiers essais, entrepris à Genève dès 1995, banques obligent !, sont plus qu'encourageants. Plusieurs sociétés, américaines (NEC et NiCT) et japonaises (JST) ont commencé à développer un produit commercial et quelques banques s'intéressent à la publicité que représenterait la protection définitive des données sensibles.

Codage dense.

L'intrication permet à Alice de communiquer deux bits d'informations à Bob en ne lui envoyant qu'un seul photon, cela s'appelle le codage dense. Cette performance ne contredit en rien l'affirmation selon laquelle tout qubit ne peut révéler in fine qu'un seul bit d'information au sens classique du terme : le codage dense implique effectivement deux photons appartenant à une même paire EPR. Mais le canal qui relie Alice à Bob n'a à en acheminer qu'un seul. Voici le principe du protocole utilisé.



Une source EPR émet deux photons intriqués sous la forme,

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

l'un vers Alice et l'autre vers Bob. Alice reçoit deux bits classiques autorisant l'encodage de 4 messages distincts, numérotés de 0 à 3, qu'elle veut pouvoir envoyer à Bob en n'envoyant

qu'un seul photon. Selon le message à transmettre, elle soumet le photon reçu à l'une des quatre transformations unitaires suivantes et renvoie le résultat à Bob :

$$0 \qquad \left|\psi_0^{'}\right\rangle = \mathrm{Id}\otimes\mathrm{Id}\left|\psi_0\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$$

$$1 \qquad \left|\psi_0^{'}\right\rangle = \mathrm{X}\otimes\mathrm{Id}\left|\psi_0\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|10\right\rangle + \left|01\right\rangle\right)$$

$$2 \qquad \left|\psi_0^{'}\right\rangle = \mathrm{Y}\otimes\mathrm{Id}\left|\psi_0\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'}\right\rangle = \frac{1}{\sqrt{2}}\left(-\left|10\right\rangle + \left|01\right\rangle\right)$$

$$3 \qquad \left|\psi_0^{'}\right\rangle = \mathrm{Z}\otimes\mathrm{Id}\left|\psi_0\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|10\right\rangle - \left|11\right\rangle\right)$$

où les opérateurs réels, I, X, Y et Z sont apparentés aux matrices de Pauli :

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathrm{Y} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Naturellement Alice n'a pu altérer que le premier qubit, celui qu'elle a reçu physiquement, l'autre est resté intact.

Lorsque Bob reçoit le photon réémis par Alice, il soumet la paire réunie dans son laboratoire à une porte c-Not. Le calcul montre que Bob peut mesurer le second qubit sans altérer le premier, en effet :

$$0 \qquad \left|\psi_0^{''}\right\rangle = \mathrm{cNot}\left|\psi_0^{'}\right\rangle \quad \Rightarrow \quad \left|\psi_0^{''}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|10\right\rangle\right)$$

$$1 \qquad \left|\psi_0^{''}\right\rangle = \mathrm{cNot}\left|\psi_0^{'}\right\rangle \quad \Rightarrow \quad \left|\psi_0^{''}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|11\right\rangle + \left|01\right\rangle\right)$$

$$2 \qquad \left|\psi_0^{''}\right\rangle = \mathrm{cNot}\left|\psi_0^{'}\right\rangle \quad \Rightarrow \quad \left|\psi_0^{''}\right\rangle = \frac{1}{\sqrt{2}}\left(-\left|11\right\rangle + \left|01\right\rangle\right)$$

$$3 \qquad \left|\psi_0^{''}\right\rangle = \mathrm{cNot}\left|\psi_0^{'}\right\rangle \quad \Rightarrow \quad \left|\psi_0^{''}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle - \left|10\right\rangle\right)$$

Si le second qubit est mesuré par Bob à la valeur '0' (resp. '1'), c'est qu'on est dans les cas 0 ou 3 (resp. 1 ou 2). Bob peut maintenant appliquer une porte de Hadamard au premier qubit et la mesure permet de trouver le message d'origine, en effet :

$$0 \qquad \left|\psi_0^{'''}\right\rangle = \mathrm{H}\frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)\left|0\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'''}\right\rangle = \left|00\right\rangle$$

$$1 \qquad \left|\psi_0^{'''}\right\rangle = \mathrm{H}\frac{1}{\sqrt{2}}\left(\left|1\right\rangle + \left|0\right\rangle\right)\left|1\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'''}\right\rangle = \left|01\right\rangle$$

$$2 \qquad \left|\psi_0^{'''}\right\rangle = \mathrm{H}\frac{1}{\sqrt{2}}\left(-\left|1\right\rangle + \left|0\right\rangle\right)\left|1\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'''}\right\rangle = \left|11\right\rangle$$

$$3 \qquad \left|\psi_0^{'''}\right\rangle = \mathrm{H}\frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)\left|0\right\rangle \quad \Rightarrow \quad \left|\psi_0^{'''}\right\rangle = \left|01\right\rangle$$

Téléportation.

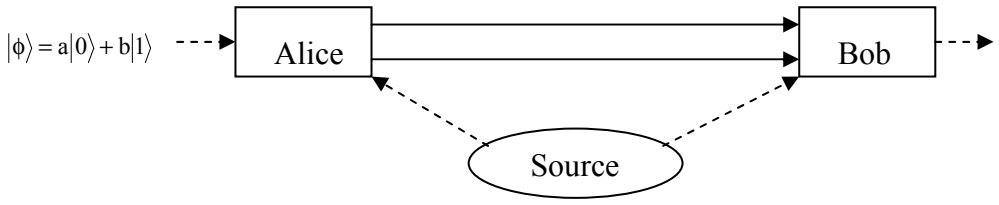
La téléportation est en un certain sens, que l'on va préciser, l'opération inverse du codage dense. Il s'agit de transmettre, par voie classique, l'information suffisante pour être en mesure de reconstruire de toute pièce et à distance un état quantique inconnu mais donné. Il va de soi que le prix à payer pour cette téléportation est la destruction de l'état quantique source sinon on aurait contrevenu au « no cloning theorem ».

Imaginons qu'Alice dispose d'un état, ϕ, qu'elle ne connaît pas mais qu'elle veut transmettre à Bob par un canal classique,

$$|\phi\rangle = a|0\rangle + b|1\rangle$$

Elle dispose pour ce faire d'un des photons d'une paire EPR dont l'autre est en possession de Bob. L'état de la paire est décrit par :

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$



Alice et Bob vont en fait inverser l'ordre des manoeuvres effectuées lors du codage dense : Alice commence par combiner les états , ϕ et ψ_0, sous la forme,

$$|\phi\rangle \otimes |\Psi_0\rangle = \frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right).$$

En se souvenant qu'elle ne contrôle que les deux premiers bits, elle soumet cet état aux transformations successives, cNot⊗Id puis H⊗Id⊗Id :

$$(H \otimes Id \otimes Id)(cNot \otimes Id)(|\phi\rangle \otimes |\Psi_0\rangle) =$$
$$\frac{1}{2}\left(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)\right)$$

Ensuite elle mesure les deux premiers bits, trouvant, avec des probabilités égales, l'une des quatre possibilités, '00', '01', '10 ou '11' mais détruisant par là même l'état à transmettre. Toutefois l'information suffisante est sauvée qui va permettre à Bob de le reconstruire à distance. En effet celui-ci va recevoir par un canal classique le résultat de la mesure d'Alice, '01' par exemple. Or il connaît la table de reconversion des bits reçus :

‘00’ $\Rightarrow$ $|\phi\rangle = \mathrm{Id}(a|0\rangle + b|1\rangle)$

‘01’ $\Rightarrow$ $|\phi\rangle = \mathrm{X}(a|1\rangle - b|0\rangle)$

‘10’ $\Rightarrow$ $|\phi\rangle = \mathrm{Z}(a|0\rangle - b|1\rangle)$

‘11’ $\Rightarrow$ $|\phi\rangle = \mathrm{Y}(a|1\rangle - b|0\rangle)$

Il suffit à Bob d’appliquer la bonne transformation au photon qu’il a reçu de la source EPR pour qu’il le projette dans l’état demandé, $|\phi\rangle = a|0\rangle + b|1\rangle$, dans tous les cas.

Le « paradoxe » EPR.

Alain Aspect

John Bell

Déterminisme ou probabilisme, réalisme ou positivisme ?

C'est intentionnellement que nous avons détaché de l'exposé principal la délicate discussion du « paradoxe » EPR et de tout ce qui tourne autour. La notion de paradoxe (de Loschmidt, de Bertrand, des jumeaux, etc…) n'a pas droit de cité en physique. C'est tout au plus un énoncé provocant qui confronte une réalité expérimentale à une intuition défaillante ou à un modèle théorique qui prend ses désirs pour des réalités. Dans tous les cas, la seule attitude raisonnable consiste à prendre acte des faits expérimentaux et de tout mettre en œuvre pour développer de nouvelles intuitions plus conformes à cette réalité. La mécanique quantique est particulièrement exigeante à cet égard mais rappelons que la relativité, même dans sa forme restreinte, l'est tout autant.

Dès 1930, la physique théorique a été secouée par un débat d'interprétations, alimenté par les points de vues contradictoires défendus par deux physiciens éminents, Einstein et Bohr.

Déterminisme ou probabilisme ?

Un noyau radioactif émet des particules, α, β ou γ, de façon complètement aléatoire. De même un photon franchit ou se réfléchit sur une lame semi transparente sans obéir à une loi apparente. Bohr a toujours admis que le probabilisme que l'on observe effectivement au niveau quantique est essentiel et irréductible à quelque cause sous-jacente que ce soit. Einstein, par contre, était convaincu que ce hasard n'est pas fondamentalement différent du comportement erratique des systèmes chaotiques et qu'un jour viendra où l'on découvrira un ensemble de variables, actuellement inconnues, dont le comportement instable est responsable du désordre observé. L'immense majorité des physiciens s'est finalement sagement rangée au point de vue de Bohr. Le refuser, c'est s'exposer à des difficultés colossales même pour expliquer une expérience aussi simple que celle de l'interféromètre de Mach-Zender. De fait, en admettant qu'il existe un mécanisme interne à la lame semi-transparente, qui distribuerait pseudo-aléatoirement les photons selon le canal réfléchi ou transmis, on ne voit pas du tout comment on concilierait ce type d'explication avec le fait qu'à la sortie de la deuxième lame de l'interféromètre correctement réglé, c'est toujours le même détecteur qui enregistre l'arrivée du photon.

Certes on peut toujours essayer d'imaginer des mécanismes de plus en plus alambiqués qui y parviendraient mais ce serait aller à l'encontre du principe d'Occam qui préconise de toujours préférer les explications simples. Décrire la réalité quantique en termes de variables cachées n'est pas forcément impossible, Bohm et son école semblent avoir été très loin dans cette direction, mais c'est compliquer inutilement les choses pour un profit nul, en tous cas à ce jour, car aucune théorie de ce genre n'a jamais expliqué ou prédit un phénomène qui aurait échappé à la théorie de Bohr. Une théorie basée sur des variables cachées ressemble beaucoup à une tentative d'insinuer que la science pourrait prouver l'existence d'un « Dieu qui ne joue pas aux dés », chose qui est hors de sa portée. Le débat n'a toutefois pas été complètement inutile en ce qu'il a fixé un certain nombre d'idées pas toujours faciles à recevoir.

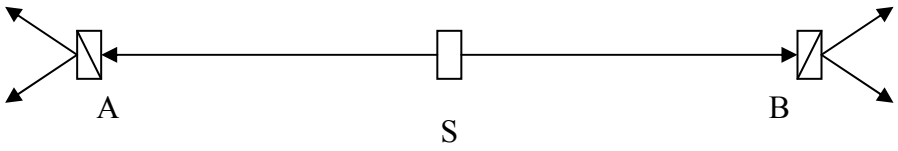
Réalisme ou positivisme ?

Le débat qui oppose le déterminisme au probabilisme n'est qu'un aspect particulier d'un débat philosophique plus large que l'on retrouve à tous les stades du développement des sciences naturelles.

Sans chercher à raffiner le sens des mots, rappelons qu'une attitude positiviste (par opposition à une attitude réaliste), en science, consiste à s'en tenir aux faits observés sans nécessairement chercher à leur trouver une explication à un niveau de profondeur accru. Cette attitude n'a pas toujours été bien considérée. Après tout, on a pu la rendre responsable du retard pris par l'émergence de l'hypothèse atomique qui collait pourtant bien à l'explication de phénomènes macroscopiques comme le mouvement brownien ou le comportement des gaz parfaits. De même, ce fut un progrès indéniable de réaliser que nombre de maladies uniquement connues par leur symptomatologie étaient, au moins en partie, la conséquence de l'existence de bactéries.

Einstein était un adepte du réalisme en physique. En particulier, il ne pouvait admettre que le monde quantique se démarque du monde macroscopique dans ses rapports avec le hasard. Dans notre monde macroscopique, il arrive que des événements, tel le fonctionnement d'une roulette de casino, semblent aléatoires mais nous savons que ce n'est que la conséquence d'un mouvement chaotique sous-jacent. Nous avons appris à reconnaître qu'un grand nombre de systèmes soumis à des lois parfaitement déterministes pouvaient donner l'illusion du hasard au point de franchir les tests statistiques les plus exigeants. Un exemple connu est fourni par l'automate cellulaire unidimensionnel portant le numéro 30 dans la nomenclature de Wolfram : en dépit de règles déterministes particulièrement simples, il est, à la satisfaction générale des utilisateurs, à la base de la fonction Random du logiciel Mathematica. Einstein était convaincu que l'aléatoire quantique était, lui aussi, réductible à un déterminisme sous-jacent devant faire l'objet d'une découverte ultérieure. Bohr n'était pas de cet avis et il pensait au contraire que l'indéterminisme à l'échelle atomique est fondamental et irréductible. En ce sens il prenait le risque de l'attitude positiviste.

L'expérience par la pensée suivante, inspirée de celle proposée pour la première fois par Einstein, Podolsky et Rosen (d'où son surnom EPR) illustre la différence des points de vue en présence.



Une source, S, de moment angulaire nul, émet des couples de particules en opposition. Ces particules emportent chacune un moment angulaire mais il ne s'agit nullement d'un moment orbital puisque l'émission se fait selon une droite passant par S. Il s'agit d'un moment de spin dont la valeur totale doit être conservée à la valeur initiale, zéro. En particulier, si l'observateur, Alice en A, mesure un spin +1/2 pour sa particule relativement à Oz, il est certain que celui situé en B, Bob, mesurera la valeur –1/2 pour la sienne par rapport au même axe. A part cette opposition certaine, les valeurs mesurées par Alice et Bob sont complètement aléatoires. Pour Bohr, adepte du positivisme, cela ne réclame aucune

explication : c'est un fait que le monde quantique est aléatoire et il n'y a pas lieu de tenter d'expliquer ou de réduire cet aléa à un mécanisme caché.

Mais pour Einstein, Dieu ne joue pas aux dés : si les particules émises par la source sont dans des états de spin aléatoires, c'est qu'il existe, dissimulé dans la source, un mécanisme caractérisé par une variable cachée, λ, susceptible de prendre plusieurs valeurs, λ_j, avec des probabilités, p_j. Le hasard observé à l'émission n'est nullement la conséquence d'un hasard caché, on n'aurait fait que déplacer le problème. Il faut plutôt comprendre que le mécanisme invoqué évolue de façon suffisamment complexe et chaotique pour donner l'illusion du hasard lorsqu'il confère leurs spins respectifs aux deux particules émises (sous la contrainte que leur somme soit nulle). Une fois les particules émises, tout est dit : elles sont séparées et transportées telles quelles vers les appareils de mesure (analyseurs de Stern-Gerlach ou polariseurs, en bref analyseurs).

La présentation usuelle du « paradoxe » EPR ainsi que son aboutissement sous la forme des expériences d'Aspect s'apparentent, avec le recul, à une tempête dans un verre d'eau. La raison en est qu'il ne s'agit, en définitive, que d'un débat d'interprétation de la théorie quantique. Or rien dans les principes axiomatiques de cette théorie ne permet de régler ce genre de problème. A cet égard, l'attitude adoptée par Feynman est exemplaire : jusqu'à preuve du contraire, le modèle quantique confirme toutes les réalités expérimentales et sauf à faire preuve de beaucoup d'entêtement, toute « tentation paradoxale » ne pourrait que renvoyer à un ensemble de préconceptions inadaptées. Cela dit, il demeure intéressant d'entrer dans le détail d'une expérience EPR : c'est une excellente façon de contrôler que l'on a assimilé les lois du monde quantique.

Une expérience EPR.

Commençons par rappeler la différence essentielle qui concerne le résultat de toute mesure tentée sur un ensemble de deux particules selon qu'elles sont intriquées ou qu'elles ne le sont pas. Considérons, par exemple, l'état séparable,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |00\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle\left(|0\rangle + |1\rangle\right) .$$

Une mesure tentée sur la première particule fournira avec certitude la valeur '0' et ce résultat n'a aucune influence sur une mesure effectuée ultérieurement sur la deuxième particule pour laquelle on trouvera '0' (ou '1') avec la probabilité 1/2. On aurait pu tout aussi bien effectuer ces deux mesures dans l'ordre inverse et rien n'aurait changé à ces prédictions. En d'autres termes, l'ordre des mesures est indifférent dans le cas séparable.

Par contre, si l'on considère l'état intriqué,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right),$$

la conclusion change radicalement : une mesure effectuée sur la première particule fournira, la valeur '0' (ou '1') avec la probabilité 1/2, mais dans ce cas toute mesure ultérieure tentée sur

la deuxième particule fournira avec certitude le résultat contraire. Naturellement, le résultat est inverse si on permute l'ordre des mesures en sorte que la commutativité n'est plus assurée dans le cas intriqué. Nous évoquerons sous peu les précautions que cette permutation dans le temps requiert au niveau de la synchronisation des horloges attachées aux observateurs.

Le protocole EPR existe dans deux variantes : l'une, plus aisée à suivre, utilise une source émettant deux particules matérielles identiques porteuses chacune d'un moment magnétique, l'autre, plus facile à mettre en œuvre expérimentalement, utilise une source émettant deux photons. Commençons par la première.

Expérience EPR utilisant des particules matérielles.

Une source au repos dans un état de spin total nul (état singulet) émet des couples de particules chargées de spin 1/2 dans des directions nécessairement opposées afin de garantir la conservation de la quantité de mouvement. Deux observateurs, Alice et Bob, disposent chacun d'un appareil de Stern-Gerlach qu'ils peuvent faire tourner autour de la direction de propagation. Le vecteur d'état qui décrit le système des deux particules au moment où elles quittent la source se note dans la base, $\left(|z+\rangle_A|z+\rangle_B, |z+\rangle_A|z-\rangle_B, |z-\rangle_A|z+\rangle_B, |z-\rangle_A|z-\rangle_B\right)$:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_A|z-\rangle_B - |z-\rangle_A|z+\rangle_B\right),$$

où l'on a tenu compte de la conservation du moment angulaire et de la parité.

Supposons qu'Alice envisage de mesurer la composante du spin de sa particule selon l'axe Oz. Pour ce faire elle aligne évidemment son analyseur selon cet axe. Si elle recommence l'expérience sur chaque particule qui lui parvient successivement, elle trouvera nécessairement, +1/2 ou –1/2, aléatoirement. Autrement dit la suite des mesures effectuées par Alice fournit une suite d'états complètement aléatoire, d'entropie 1bit/symb, du style :

$$|z-\rangle_A|z-\rangle_A|z+\rangle_A|z-\rangle_A|z+\rangle_A|z-\rangle_A|z+\rangle_A|z-\rangle_A|z+\rangle_A|z+\rangle_A|z-\rangle_A|z-\rangle_A|z-\rangle_A|z+\rangle_A\cdots$$

Intéressons-nous à présent à la suite des mesures effectuées par Bob sur l'ensemble des particules qui lui parviennent. Bob n'est absolument pas obligé d'orienter son analyseur comme l'a fait Alice. Posons, en toute généralité, que son appareil fait un angle, θ_{AB}, avec celui d'Alice. Nous connaissons les lois de transformations des vecteurs d'états lorsque les axes tournent autour de Oy :

$$|z'+\rangle_B = \cos\frac{\theta_{AB}}{2}|z+\rangle_B + \sin\frac{\theta_{AB}}{2}|z-\rangle_B \quad \Leftrightarrow \quad |z+\rangle_B = \cos\frac{\theta_{AB}}{2}|z'+\rangle_B - \sin\frac{\theta_{AB}}{2}|z'-\rangle_B$$

$$|z'-\rangle_B = -\sin\frac{\theta_{AB}}{2}|z+\rangle_B + \cos\frac{\theta_{AB}}{2}|z-\rangle_B \quad \Leftrightarrow \quad |z-\rangle_B = \sin\frac{\theta_{AB}}{2}|z'+\rangle_B + \cos\frac{\theta_{AB}}{2}|z'-\rangle_B$$

Si Alice n'avait effectué aucune mesure préalable, il va de soi que Bob aurait trouvé, lui aussi, une suite de mesures complètement aléatoire donc incompressible, du style,

$$|z'+\rangle_B|z'-\rangle_B|z'+\rangle_B|z'+\rangle_B|z'+\rangle_B|z'-\rangle_B|z'+\rangle_B|z'-\rangle_B|z'-\rangle_B|z'-\rangle_B|z'-\rangle_B|z'+\rangle_B|z'-\rangle_B\cdots$$

Intéressons-nous, à présent, au cas où Alice a effectué une mesure préalable. Une fois sur deux, en moyenne, elle détecte l'état, $|z+\rangle_A$, ce qui a eu pour effet de faire basculer instantanément le système dans l'état,

$$|\psi_I\rangle = |z+\rangle_A |z-\rangle_B = |z+\rangle_A \left(\sin\frac{\theta_{AB}}{2} |z'+\rangle_B + \cos\frac{\theta_{AB}}{2} |z'-\rangle_B \right).$$

L'autre fois sur deux, elle détecte, $|z-\rangle$, ce qui fait basculer le système dans l'état,

$$|\psi_I\rangle = |z-\rangle_A |z+\rangle_B = |z-\rangle_A \left(\cos\frac{\theta_{AB}}{2} |z'+\rangle_B - \sin\frac{\theta_{AB}}{2} |z'-\rangle_B \right).$$

Lorsque Alice et Bob auront chacun effectué leur mesure, le système se trouvera obligatoirement avec une probabilité définie dans l'un des quatre états suivants :

$|z+\rangle_A |z'+\rangle_B$, avec la probabilité, $\frac{1}{2}\sin^2(\theta_{AB}/2)$,
$|z+\rangle_A |z'-\rangle_B$, avec la probabilité, $\frac{1}{2}\cos^2(\theta_{AB}/2)$,
$|z-\rangle_A |z'+\rangle_B$, avec la probabilité, $\frac{1}{2}\cos^2(\theta_{AB}/2)$,
$|z-\rangle_A |z'-\rangle_B$, avec la probabilité, $\frac{1}{2}\sin^2(\theta_{AB}/2)$.

On constate que quelle que soit la valeur de θ_{AB}, la suite des mesures effectuées par Bob est tout aussi aléatoire que la suite des mesures effectuées par Alice. Bob est donc parfaitement incapable de décider si Alice a ou n'a pas effectué de mesure préalable sur ses particules. Par contre, une différence apparaît en fonction de l'angle si Alice et Bob comparent leurs listes respectives. Ils peuvent définir un facteur de corrélation, Γ, entre ces listes de longueur, N, par la formule :

$$\Gamma = \frac{1}{N} \sum_{1}^{N} \text{sign}(\text{mes}_A) \ \ \text{sign}(\text{mes}_B).$$

En particulier, si l'expérience est recommencée un grand nombre, N, de fois,

- Si θ_{AB} est nul, Bob trouvera systématiquement une composante de spin de signe opposé à celle trouvée par Alice, on dit qu'il y a anticorrélation parfaite, $\Gamma = -1$.

- Si θ_{AB} vaut 180°, Bob trouvera systématiquement une composante de spin de même signe que celle trouvée par Alice, on dit qu'il y a corrélation parfaite, $\Gamma = +1$.

- Si θ_{AB} vaut 90°, Bob trouvera systématiquement une composante de spin totalement indépendante de celle trouvée par Alice, on dit qu'il y a décorrélation parfaite, $\Gamma = 0$.

- Dans tous les autres cas la corrélation est partielle, $\Gamma = -\cos\theta_{AB}$.

Insistons sur quelques conséquences qui contrarient tellement l'intuition qu'elles ont provoqué le débat initié par Einstein en personne. Einstein ne voyait pas ce qui pourrait empêcher Alice et Bob de procéder l'une, Alice, à la mesure de S_z et l'autre, Bob, à la mesure de S_x, c'est le cas, $\theta_{AB} = 90°$, évoqué il y a un instant. Chacun noterait la valeur obtenue dans son calepin et pourrait confronter les valeurs obtenues lors d'une rencontre ultérieure. Les deux particules étant émises avec un spin total nul, si Alice trouve $S_z = +1/2$, elle sait que Bob trouvera en toute certitude $-1/2$ s'il mesure également S_z. De même, si Bob mesure la composante S_x de sa particule et trouve une valeur, $+1/2$ ou $-1/2$, il en déduira qu'Alice mesurera une composante S_x de signe contraire : il semblerait qu'on aboutisse à cette situation ou deux grandeurs, S_z et S_x, qui ne commutent pas auraient été mesurées simultanément ce qui serait contraire au principe d'incertitude.

Voici où la mécanique quantique situe la faille dans ce raisonnement. La première mesure, peu importe qu'elle soit faite par Alice ou par Bob, modifie le système des deux particules intriquées, en sorte que la deuxième mesure ne concerne plus du tout le même système qui a d'ailleurs cessé d'être intriqué. Si Alice et Bob répètent l'expérience précédente un grand nombre de fois et qu'ils confrontent leurs listes de mesures, ils s'aperçoivent qu'ils n'ont nullement mis le principe d'incertitude en défaut : toutes les fois qu'Alice aura mesuré $S_z = +1/2$, Bob aura mesuré un S_x fluctuant aléatoirement une fois sur deux de $+1/2$ à $-1/2$ car la corrélation est nulle dans ce cas, $\Gamma = 0$. On pourrait se demander ce qu'il faudrait penser du cas où les deux mesures se feraient parfaitement simultanément. Cette éventualité n'a pas à être prise en considération ni au plan expérimental, pour des raisons évidentes, ni même au plan théorique car c'est cette fois la relation d'incertitude temps–énergie qui prend le relais interdisant de fixer la coordonnées temporelle des événements avec une précision infinie.

Dans l'expérience précédente, rien n'empêche Alice et Bob d'être éloignés d'une distance, d, arbitrairement grande y compris du « genre espace » c'est-à-dire telle que, $d > c\Delta t$, où Δt représente l'intervalle temporel qui sépare la mesure d'Alice de celle de Bob. Dans ce cas, on a établi une action à distance qui ne respecte pas le principe de séparabilité relativiste selon lequel deux événements trop éloignés dans l'espace-temps ne peuvent entretenir de relation causale. C'est un fait établi que le monde quantique n'obéit pas au principe de séparabilité.

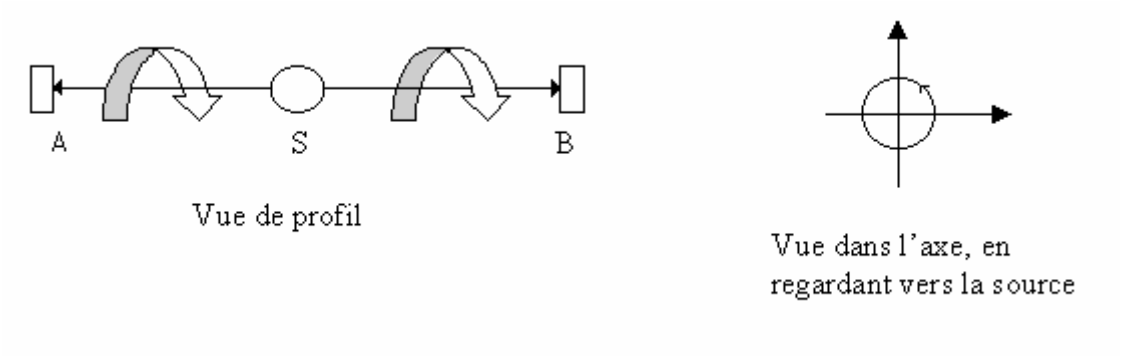
Il importe de remarquer que l'on n'a pas trouvé pour autant le moyen de communiquer une information instantanément à distance : certes le double du message mesuré par Alice (ou son contraire) peut être instantanément communiqué à Bob, lorsque $\theta_{AB} = 0°$ (ou 180°), mais ce message est complètement aléatoire. Autant demander à Bob de jouer lui-même directement à pile ou face. Tout au plus peut-on y voir le moyen de communiquer, de façon non sécurisée, un code de chiffrement aléatoire mais certainement pas un message prédéterminé.

Expérience EPR utilisant des photons.

La même expérience peut être tentée avec des photons, deux polariseurs doivent simplement remplacer les analyseurs de Stern-Gerlach. Les calculs sont identiques sauf que dans les formules de changement de base, l'angle doit être doublé.

On considère une paire de photons issus de la désintégration d'un atome de spin nul et émis en opposition par rapport à la source. Les composantes de leurs spins selon l'axe, Oz, qui joint les sources, sont obligatoirement en opposition sinon la loi de conservation du moment cinétique serait violée. Pour les deux observateurs, Alice et Bob, qui regardent la source, ces photons apparaissent de polarisations circulaires identiques (gauches sur la figure) mais par rapport à un axe Oz unique, ces polarisations sont inverses. Le vecteur d'état du système représenté ci-dessous s'écrit dans la base naturelle :

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle|z-\rangle + |z-\rangle|z+\rangle\right) = \frac{1}{\sqrt{2}}\left(|R\rangle|L\rangle + |L\rangle|R\rangle\right)$$



Expérimentalement, il est plus commode d'analyser l'état des photons relativement à la base $(|x\rangle, |y\rangle)$ qui correspond aux états de polarisation linéaire. Vu que l'on a :

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + i|y\rangle\right)$$
$$|L\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle - i|y\rangle\right)$$,

on trouve que l'état des photons peut être réécrit sous la forme :

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle_A|x\rangle_B + |y\rangle_A|y\rangle_B\right).$$

Alice et Bob peuvent mesurer les états de polarisation linéaire de leur photon respectif en interposant un cristal de calcite qui a pour effet de séparer physiquement les trajectoires des photons polarisés selon Ox et ceux polarisés selon Oy. Les règles de la mécanique quantique prédisent et l'expérience vérifie que, quel que soit le nombre de fois que l'on recommence l'expérience, lorsque Alice effectue sa mesure en premier, elle trouve un photon canalisé selon 'x' ou selon 'y' aléatoirement. Lorsqu'elle trouve, 'x', (resp. 'y'), il est certain que Bob mesurera ultérieurement que son photon est canalisé selon 'x' (resp. 'y'). La situation est inversée si c'est Bob qui mesure en premier. La théorie quantique interprète ces

faits en posant que la première mesure projette l'état du système sur $|x\rangle_A|x\rangle_B$ ou sur $|y\rangle_A|y\rangle_B$ selon le cas. La deuxième mesure peut être faite ou ne pas être faite, de toutes façons elle ne modifiera plus le vecteur d'état ainsi projeté. L'usage est largement répandu, dans la littérature, de qualifier d'instantanée la projection du vecteur d'état lors de la première mesure. Cette affirmation ne peut se faire sans précautions : le compte rendu de toute expérience où la variable temps joue un rôle exige que l'on s'assure du bon synchronisme des horloges utilisées. Lorsqu'on affirme que la mesure effectuée par Alice conditionne instantanément toute mesure effectuée par Bob cela ne peut signifier qu'une chose : c'est que le conditionnement dont il est question ne prend cours qu'au moment précis où l'horloge locale de Bob affiche la même indication horaire que celle d'Alice affichait au moment de sa mesure. Il se fait que les deux photons émis simultanément par la source réalisent automatiquement la synchronisation requise des horloges.

Rien n'oblige Alice et Bob à aligner les directions passantes de leurs polariseurs respectifs selon les mêmes axes Ox et Oy. Voyons ce qui se passe si Bob choisit de les orienter selon Ox' et Oy', faisant un angle θ_{AB} avec les précédents. Alice commence par faire une mesure de la polarisation linéaire du photon qu'elle reçoit selon son système d'axes, Ox et Oy. Elle trouve une polarisation selon Ox (ou Oy) en moyenne une fois sur deux. Convenons de ne nous intéresser qu'aux cas où Alice détecte une polarisation selon Ox. Le système bascule instantanément dans l'état particulier,

$$|\psi_I\rangle \underset{\text{renorm}}{=} |x\rangle_A|x\rangle_B .$$

Voyons à présent, à quoi on doit s'attendre si Bob fait, à son tour, le mesure de la polarisation du photon qu'il reçoit avec des polariseurs dont les directions passantes, Ox' et Oy', sont inclinées sous l'angle θ_{AB}. Nous connaissons les relations de changement de base pour passer des axes (Ox, Oy) aux axes (Ox',Oy') :

$$|x'\rangle_B = \cos\theta_{AB}|x\rangle_B + \sin\theta_{AB}|y\rangle_B \quad \Leftrightarrow \quad |x\rangle_B = \cos\theta_{AB}|x'\rangle_B - \sin\theta_{AB}|y'\rangle_B$$
$$|y'\rangle_B = -\sin\theta_{AB}|x\rangle_B + \cos\theta_{AB}|y\rangle_B \quad \Leftrightarrow \quad |y\rangle_B = \sin\theta_{AB}|x'\rangle_B + \cos\theta_{AB}|y'\rangle_B$$

d'où on déduit le vecteur d'état dans cette nouvelle base :

$$|\psi_I\rangle = |x\rangle_A \left(\cos\theta_{AB}|x'\rangle_B - \sin\theta_{AB}|y'\rangle_B\right).$$

Lorsque Alice et Bob auront chacun effectué leur mesure, le système se trouvera obligatoirement avec une probabilité définie dans l'un des quatre états suivants :

$|x\rangle_A|x'\rangle_B$, avec la probabilité, $\frac{1}{2}\cos^2\theta_{AB}$,

$|x\rangle_A|y'\rangle_B$, avec la probabilité, $\frac{1}{2}\sin^2\theta_{AB}$,

$|y\rangle_A|x'\rangle_B$, avec la probabilité, $\frac{1}{2}\sin^2\theta_{AB}$,

$|y\rangle_A|y'\rangle_B$, avec la probabilité, $\frac{1}{2}\cos^2\theta_{AB}$.

On voit que les probabilités que B détecte son photon polarisé selon Ox' (resp. Oy') valent respectivement $\cos^2 \theta_{AB}$ et $\sin^2 \theta_{AB}$. Dans ce qui suit, nous optons pour la convention suivante : on associe la valeur +1 à une polarisation selon Ox et la valeur –1 à une polarisation selon Oy. Examinons de plus près quelques cas particuliers importants :

- Si θ_{AB} est nul, Bob trouvera systématiquement une polarisation identique à celle trouvée par Alice, on dit qu'il y a corrélation parfaite, $\Gamma = 1$.

- Si θ_{AB} vaut 90°, Bob trouvera systématiquement une polarisation contraire à celle trouvée par Alice, on dit qu'il y a anticorrélation parfaite, $\Gamma = -1$.

- Si θ_{AB} vaut 45° (ou 135°), Bob trouvera systématiquement une composante de spin totalement indépendante de celle trouvée par Alice, on dit qu'il y a décorrélation parfaite, $\Gamma = 0$.
- Pour toute autre valeur de l'angle, la corrélation est partielle, $\Gamma=\cos(2\theta_{AB})$.

En 1930, ce scénario expérimental n'était qu'une expérience par la pensée. Einstein n'a de fait pas connu le verdict d'une expérience qui ne sera réalisée que 20 ans après sa disparition. On peut légitimement se demander s'il se serait-il accroché à l'idée que l'état des photons est définitivement fixé une fois qu'ils ont quitté la source ? Les expériences d'Aspect, tentées avec succès de 1976 à 1983 sur des paires de photons intriqués vérifient les prédictions de la mécanique quantique, en particulier le facteur de corrélation en $\Gamma = -\cos(2\theta_{AB})$. Elles continuent de fonctionner, avec les mêmes résultats, si on choisit les directions des polariseurs après l'émission des photons par la source. Certes le montage expérimental doit prévoir un temps de réaction des polariseurs très court mais un système de commutateurs réagissant à 10^{-8} s suffit pour y parvenir. Ce système enfreint manifestement le principe de séparabilité relativiste.

On dit souvent des systèmes quantiques intriqués qu'ils obéissent à une physique non locale où le terme local doit être compris comme l'antonyme de global. Autrement dit les systèmes quantiques intriqués se comportent comme un objet unique quel que soit le degré de d'éloignement de chacune de leurs parties. Il n'est peut-être pas indispensable de chercher de nuances significatives entre séparabilité et non-localité, c'est en tous cas l'avis d'Aspect, et le fait est que nous suivrons son conseil. En résumé, l'inséparabilité est une propriété des systèmes quantiques intriqués qu'ils entretiennent, quelle que soit la distance qui les sépare, aussi longtemps que le milieu ambiant ne les décohère pas.

Ce débat est clos : le principe de non-séparabilité est maintenant largement admis par la communauté des physiciens. Ceci devrait donc constituer la fin de l'histoire : un modèle, la mécanique quantique, décrit correctement toutes les situations expérimentales auxquelles elle a été confrontée jusqu'à présent. Que vouloir de plus ? Par contre, rien dans ce qui précède ne tranche le débat qui tourne autour du déterminisme. On a voulu aller plus loin et tordre définitivement le cou à l'idée déterministe selon laquelle l'état apparemment aléatoire des photons qui quittent la source est, en réalité, fixé par les valeurs de quelque(s) paramètre(s) hautement instables caché(s) dans cette source. L'argumentation développée par Bell va dans ce sens. Nous la présentons brièvement assortie de quelques remarques critiques soulevées par les tenants irréductibles du déterminisme.

L'argument de Bell.

La présentation habituelle de l'argumentation développée par Bell repose sur un ensemble d'inégalités qui portent son nom, que tout modèle à variables cachées est sensé devoir respecter et que l'expérience contredit. Nous nous contenterons d'une seule d'entre elles.

En supposant qu'Einstein ait connu les résultats des expériences d'Aspect et qu'il ait persévéré dans son idée fixe, il n'aurait pas manqué de chercher un modèle à variables cachées capables de restituer la corrélation observée en $\Gamma = -\cos\theta_{AB}$. Bell fut le premier à montrer que c'est peine perdue du moins si l'on accepte quelques hypothèses « raisonnables » sur lesquelles nous aurons à revenir.

Le raisonnement qui suit reprend le principe de l'expérience EPR effectuée avec des particules magnétiques. Nous faisons ce choix parce que la discussion se fait directement en terme de spins + et -. De toutes façons, les calculs sont identiques avec des photons sauf qu'il faut doubler les angles dans ce cas.

Le raisonnement de Bell se fait par l'absurde : il pose l'hypothèse que la valeur de la variable cachée, λ, conditionne le spin de chaque particule à l'émission puis il montre que les conséquence sont incompatibles avec ce que l'expérience révèle. Cette variable, à l'évolution essentiellement chaotique, peut prendre un ensemble de valeurs discrètes, $\{\lambda_i\}$, en respectant la distribution de probabilités, $\{p_i\}$. Bien entendu, l'orientation des analyseurs a aussi son mot à dire au moment de la mesure et Bell admet que cela se fait dans le respect du principe de localité : le résultat de la mesure faite à gauche (resp. à droite) ne dépend que de la valeur de λ et de celle de l'angle de l'analyseur correspondant, θ_A (resp. θ_B) mais pas de l'orientation de l'analyseur d'en face :

$$\alpha=X_G(\theta_A,\lambda) \qquad \text{et} \qquad \beta=X_D(\theta_B,\lambda) \qquad (\alpha,\beta=\pm 1).$$

Le facteur de corrélation entre les mesures se calcule aisément, il vaut :

$$\Gamma=\sum_j p_j X_G(\theta_A,\lambda_j)X_D(\theta_B,\lambda_j).$$

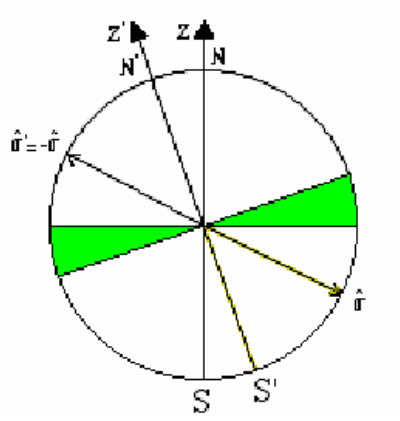
Rien n'oblige la variable cachée à ne prendre que des valeurs discrètes. Dans le cas continu, il suffit d'introduire la densité de probabilité correspondante, $\rho(\lambda)$, puis d'écrire :

$$\Gamma=\int \rho(\lambda)X_G(\theta_A,\lambda)X_D(\theta_B,\lambda)d\lambda \qquad (\rho(\lambda)\geq 0,\ \int\rho(\lambda)d\lambda=1).$$

Pour des raisons de symétrie évidentes, seule doit compter la différence entre les angles θ_A et θ_B que nous notons, $\theta_{AB}= \theta_B-\theta_A$. Et voilà que les ennuis commencent car la forme « à variables angulaires séparées » précédente ne se réduit pratiquement jamais à une fonction de la différence des angles et jamais à la forme particulière convoitée, $\Gamma = -\cos\theta_{AB}$. Le modèle géométrique suivant donne une idée de ce qui se passe.

Il consiste à poser l'existence d'un vecteur unitaire caché, $\hat{\sigma}$, qui encode l'orientation du spin des particules dès leur sortie de la source. Les analyseurs sont, quant à eux,

caractérisés chacun par la direction NS de leur gradient magnétique. On pose qu'Alice mesurera $|z+\rangle$ (resp. $|z-\rangle$) toutes les fois que $\lambda = \hat{\sigma}\cdot\hat{z} > 0$ (resp. $\lambda<0$) et la même chose pour Bob en remplaçant $\hat{\sigma}$ par $\hat{\sigma}' = -\hat{\sigma}$ et $\hat{z}$ par $\hat{z}'$. En termes géométriques, l'orientation de $\hat{\sigma}$ est aléatoire au niveau de la source et c'est l'équateur correspondant à la direction NS de chaque analyseur qui fixe le résultat de la mesure. Autrement dit, la mesure donnera $|z+\rangle$ ou $|z-\rangle$ selon que $\hat{\sigma}$ tombe dans l'hémisphère nord ou sud.



Dire que l'orientation de $\hat{\sigma}$ est aléatoire signifie l'équiprobabilité de ses orientations possibles entre 0 et 2π. Calculons le facteur de corrélation, Γ, dans le cadre de ce modèle. Une manière savante de procéder consiste à reconnaître que dans l'expression générale,

$$\Gamma = \int \rho(\lambda) X_G(\theta_A,\lambda) X_D(\theta_B,\lambda) d\lambda$$

il suffit de prendre pour λ l'angle que $\hat{\sigma}$ fait avec Oz et de poser :

$$X_G(\lambda,\theta_A) = \text{sign}[\cos(\theta_A - \lambda)] \qquad X_D(\lambda,\theta_B) = \text{sign}[\cos(\theta_B - \lambda)]$$

et

$$\rho(\lambda) = \frac{1}{2\pi} \qquad (\lambda \in (0,2\pi)),$$

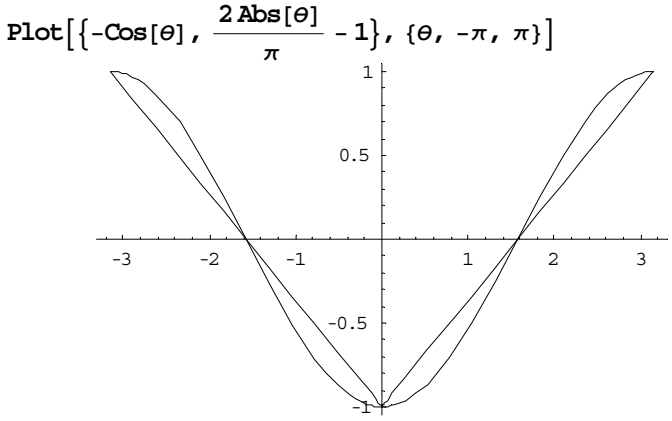
puis d'effectuer le calcul de Γ.

Une approche plus naïve mais équivalente consiste à comptabiliser les résultats possibles des mesures combinées d'Alice et de Bob. Les signes de leurs mesures coïncident lorsque $\hat{\sigma}$ tombe dans la zone sombre soit en moyenne $|\theta|$ fois sur π. La probabilité correspondante vaut donc $\frac{|\theta|}{\pi}$. De même les signes des mesures diffèrent avec la probabilité, $1 - \frac{|\theta|}{\pi}$.

Le facteur de corrélation vaut donc :

$$\Gamma=\frac{|\theta|}{\pi}-\left(1-\frac{|\theta|}{\pi}\right)=2\frac{|\theta|}{\pi}-1,$$

dont voici le graphe, superposé à celui, en –cosθ, de la prédiction quantique :



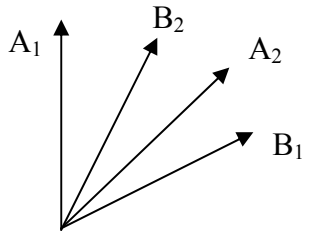
Ce modèle simple, à variables cachées, ne restitue la prédiction quantique qu'en quatre points (les extrémités se rejoignent). Pour toutes les autres valeurs de l'angle, θ_{AB}, un écart existe et seule une confrontation expérimentale peut trancher entre les deux modèles. Le problème qui se pose aux expérimentateurs est que cet écart est minime et qu'il est impossible de réaliser un test dont les barres d'erreurs ne recouvriraient pas les deux courbes. Il faut donc trouver autre chose.

Bell n'a pas fourni de démonstration directe de l'impossibilité,

$$\Gamma=\int \rho(\lambda)X_G(\theta_A,\lambda)X_D(\theta_B,\lambda)d\lambda \neq -\cos(\theta_B-\theta_A),$$

seul Feynman a été un peu plus explicite dans un article célèbre (« Simulating physics with computers, J. of Theoretical Physics, Vol21 n°6/7, 1982) où il précise, sans démonstration, que c'est l'exigence, $\rho(\lambda) \geq 0$, qui en est responsable.

Bell a préféré montrer qu'en compliquant le protocole expérimental, on pouvait amplifier l'écart entre les prédictions classique et quantique au point de rendre cette démonstration superflue. Il suffit de recommencer la même expérience quatre fois en positionnant les analyseurs de Bob et Alice dans deux orientations distinctes, A_1 et A_2, d'une part et B_1 et B_2, d'autre part, orientés par exemple comme suit :



Selon le cas dans lequel on se trouve les mesures fourniront les signes :

α_1 et β_1 si on choisit les orientations A_1 et B_1,
α_2 et β_2 si on choisit les orientations A_2 et B_2,
α'_1 et β'_2 si on choisit les orientations A_1 et B_2,
α'_2 et β'_1 si on choisit les orientations A_2 et B_1.

Si le système était séparable en deux particules qui s'ignorent après s'être quittées, on ne devrait voir aucune différence entre les α et les α' (ni entre les β et les β'). Il en résulterait que la valeur moyenne de la fonction de corrélation suivante, astucieusement choisie pour une propriété qui apparaîtra sous peu,

$$\langle\gamma\rangle=\langle\alpha_1\beta_1\rangle+\langle\alpha_1\beta_2\rangle+\langle\alpha_2\beta_1\rangle-\langle\alpha_2\beta_2\rangle=\Gamma_{11}+\Gamma_{12}+\Gamma_{21}-\Gamma_{22}$$

devrait obligatoirement naviguer entre les valeurs extrêmes –2 et +2, c'est l'inégalité de Bell :

$$-2\le\langle\gamma\rangle\le 2\ .$$

Elle résulte du fait arithmétique que chaque quantité, Γ_{ij}, est, de par sa définition, obligatoirement comprise entre les valeurs, +1 ou –1. On peut aussi vérifier le résultat annoncé sur l'exemple géométrique considéré.

La prédiction quantique ne satisfait pas l'inégalité de Bell. Il suffit pour le voir de recalculer $\langle\gamma\rangle$ en se basant sur un facteur de corrélation valant :

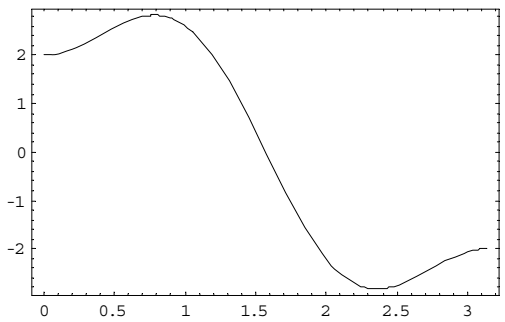
$$\Gamma_{ij}=-\cos(\theta_j-\theta_i)\ .$$

Si on effectue ce calcul avec une configuration des polariseurs qui respecte un angle identique, θ, entre A_1 et B_2, puis B_2 et A_2 et enfin entre A_2 et B_1 on trouve :

$$\langle\gamma\rangle=3\cos(\theta)-\cos(3\theta)\ ,$$

dont le graphe s'écarte maximalement de l'intervalle (-2, +2) pour un angle, θ, valant 45°.

```
Plot[3Cos[θ]-Cos[3θ],{θ,0,π},Axes→False,Frame→True]
```



L'écart est cette fois suffisamment important pour qu'une expérience même imparfaite, en particulier au niveau des comptages des coïncidences photoniques en A et en B, soit capable de trancher entre le respect ou le non-respect de l'inégalité de Bell. Le fait est que l'inégalité est violée et que la non-séparabilté du système est établie. On réalise, en pasant, l'intérêt du choix effectué pour la fonction $\langle\gamma\rangle$: une autre fonction n'aurait pas fourni un écart aussi significatif.

Si l'expérience est réalisée avec des photons, il y a lieu de doubler l'angle dans la fonction de corrélation :

$$\langle\gamma\rangle = 3\cos(2\theta) - \cos(6\theta),$$

et la violation maximale de l'inégalité de Bell devrait se produit pour un angle de 22.5°.

Naturellement, puisque ce montage est une combinaison de quatre configurations équivalentes et que la contradiction est présente à la sortie, c'est que le vers était déjà dans la pomme dès le départ. C'est bien ce que nous avons annoncé depuis le début de ce paragraphe : au plan théorique tout le problème est déjà présent dans le facteur de corrélation en, Γ=-cosθ, qu'aucune théorie à variables cachées locales ne peut reproduire. Le raisonnement de Bell peut paraître tortueux mais c'est la manière qu'il a trouvée de faire coup double en évitant une démonstration délicate et en amplifiant la divergence entre les modèles classique et quantique.

Le modèle géométrique simple que nous avons présenté est un exemple d'un modèle à variables cachées qui échoue à expliquer la réalité expérimentale. On pourrait objecter que d'autres modèles plus sophistiqués pourraient peut-être réussir là où le précédent a échoué et c'est effectivement l'espoir qu'entretiennent les tenants irréductibles d'une vision déterministe. Il y a naturellement un prix à payer pour cela. Une façon de saboter la démonstration de Bell est de prendre en considération le fait que la densité de probabilité, $\rho(\lambda)$, puisse dépendre de l'angle que font les analyseurs.

Les combats d'arrière-garde.

Si personne ne met en doute le résultat des expériences d'Aspect ni le fait que la mécanique quantique prédit correctement ce que l'on observe, il s'est trouvé des auteurs et non des moindres (Jaynes en particulier) pour contester l'usage que le raisonnement de Bell fait de la notion de probabilité. Personne n'a mis plus clairement la critique en perspective générale qu'Harthong. Son raisonnement vaut la peine d'être présenté.

Le raisonnement qui a conduit Bell à l'inégalité qui porte son nom est riche en hypothèses inexprimées. En particulier, Harthong a fait remarquer qu'il s'écroule dès l'instant où, dans le calcul de Γ, on renonce à l'indépendance des p_i (où de $\rho(\lambda)$ dans le cas continu) vis-à-vis de l'angle θ_{AB}. Il est allé plus loin en montrant que, dans l'exemple géométrique étudié, on retrouve la prédiction quantique, avec une variable cachée, si on opte pour une pondération en, $-\cos\theta_{AB}$! Voyons cela de plus près.

Lorsque, dans le modèle géométrique en question, on a recensé les cas possibles (mesures de même signes et de signes contraires), et qu'on leur a attribué les probabilités respectives, $\frac{|\theta|}{\pi}$ et $1-\frac{|\theta|}{\pi}$, on a implicitement considéré que les orientations du vecteur $\hat{\sigma}$ sont équiprobables. Mais il suffirait de remplacer cette hypothèse par une autre, à savoir que ce sont les projections de $\hat{\sigma}$ sur l'axe de mesure de chaque analyseur local qui sont équiprobables, pour que la prédiction classique rejoigne la prédiction quantique. En effet, les probabilités, $\frac{|\theta|}{\pi}$ et $1-\frac{|\theta|}{\pi}$, sont alors respectivement remplacées par $(1-\cos\theta)/2$ et $(1+\cos\theta)/2$ et on retrouve la prédiction quantique,

$\Gamma=(1-\cos\theta)/2-(1+\cos\theta)/2=-\cos\theta$.

Cette hypothèse peut surprendre mais elle est cependant dans la droite ligne de l'usage que l'on fait habituellement du calcul des probabilités. Rappelons que ce calcul n'indique nulle part dans ses axiomes comment détecter les épreuves équiprobables d'un problème donné. Poser cette équiprobabilité a priori en la tirant de son chapeau n'est pas sans danger : c'est la porte ouverte à toutes sortes de mésaventures dont le paradoxe de Bertrand est l'exemple le plus fameux. L'école de Jaynes préconise plutôt qu'on procède à une expérience statistique et qu'on en tire a posteriori la distribution des probabilités des épreuves par application du principe de l'entropie maximum.

Au lieu de poser arbitrairement, comme le fait Bell, l'indépendance des occurrences du paramètre caché par rapport à l'angle θ_{AB} et d'en tirer des conséquences en contradiction avec l'expérience, on pourrait prétendre opérer à l'inverse et déduire cette dépendance du résultat des expériences d'Aspect.

Reste à voir si cela a un sens « physique » d'admettre ce type de dépendance. Après tout, cela signifierait ni plus ni moins que l'orientation des analyseurs influence la probabilité d'occurrence de la valeur de λ qui émerge lors de la désexcitation de la source ! Si cela peut paraître absurde d'un point de vue classique, il est par contre tout à fait dans l'esprit de l'interprétation non locale de Bohr de considérer que source et détecteurs ne forment qu'un seul et même système en sorte que l'orientation des analyseurs brise la symétrie de l'espace qui serait vide sans eux. Ainsi on aperçoit, à ce stade, que toute tentative d'interpréter les phénomènes quantiques d'un point de vue déterministe n'est pas forcément vouée à l'échec pourvu qu'elle reconnaisse le caractère non local des phénomènes étudiés.

On pourrait objecter que cette interprétation déterministe se heurterait malgré tout au fait que l'expérience d'Aspect continue de fonctionner si on modifie l'orientation des analyseurs après l'émission des particules. Il faudrait en effet admettre que, dans une vision classique des choses où le spin des particules est fixé dès l'émission par la source, celle-ci subirait une rétroaction dans le temps de la part des détecteurs ! L'interprétation quantique orthodoxe ne connaît pas ces étrangetés : l'invocation, $\lambda = \lambda_j$, est un non-événement en ce sens qu'il n'a laissé aucune trace objective au niveau de la source et que ce n'est qu'au moment de la mesure que le système est fixé sur son sort. N'est-ce pas la leçon de la théorie quantique que de n'accorder de crédit qu'aux résultats des mesures ? Tout cela est déjà bien présent dans l'expérience des fentes d'Young : il n'est pas question de raisonner à partir de la traversée de telle ou elle fente car rien au niveau de celles-ci n'est venu objectiver ce passage. Et il est bien connu que si on tente précisément de l'objectiver par une détection qui laisse une

trace mesurable au niveau d'une de ces fentes, on perturbe le système au point de faire disparaître les franges d'interférence.

On voit comme ces problèmes d'interprétation sont délicats à traiter et combien il est sage d'épouser le point de vue de Bohr et de Feynman consistant à s'en tenir au positivisme de la théorie quantique. L'argument de Bell rend définitivement illusoire toute tentative d'une théorie quantique à variables cachées locales. Il n'écarte par contre pas toute perspective d'une théorie à variables cachées non locales. A ce train, les tenants du déterminisme pourront sans doute repousser sans cesse l'échéance du jour où il deviendra clair pour tout le monde que le probabilisme quantique est essentiel.

Il est juste de dire que les problèmes liés à l'interprétation de la théorie quantique ne concernent qu'une minorité de physiciens. Les pragmatiques considèrent que tant que la théorie quantique dans sa forme actuelle donne satisfaction ils ne voient pas pourquoi ils en changeraient et les sceptiques auront toujours beau jeu de prétendre qu'aucune théorie ne possède le pouvoir d'imposer une interprétation particulière d'où il s'en suit que le débat initié par Einstein ne possède pas d'issue définitive.

Complément : l'état GHZ.

On trouve des situations de type EPR dans tout système intriqué. Greenberger, Horen et Zeilinger ont récemment mis en évidence expérimentalement une telle situation dans un système à trois qubits photoniques. La même expérience a également été tentée avec succès sur des atomes. L'étrangeté du monde quantique y apparaît plus évidente que jamais.

Un état GHZ est du type intriqué suivant :

$$|\psi\rangle = \frac{1}{2}\left(|000\rangle_{ABC} - |110\rangle_{ABC} - |101\rangle_{ABC} - |011\rangle_{ABC}\right).$$

Six portes logiques sont nécessaires pour le construire à partir de l'état de base, $|000\rangle_{ABC}$, lui-même facile à fabriquer par simple filtrage :

$$|\psi\rangle = Z_B C_{CB} H_C C_{CB} C_{CA} H_C |000\rangle_{ABC}.$$

Imaginons que nous procédons à une mesure de chacun des qubits dans un ordre quelconque. Au terme des trois mesures, on est certain d'avoir trouvé une des quatre possibilités : $|000\rangle_{ABC}$, $|110\rangle_{ABC}$, $|101\rangle_{ABC}$ ou $|011\rangle_{ABC}$ à l'exclusion des quatre autres. Ces quatre états permis ont un point commun : les mesures, x_A, x_B et x_C satisfont la « loi de conservation »,

$$x_A \oplus x_B \oplus x_C = 0.$$

(Pour rappel, la table de $\oplus$ = Xor se note : $0 \oplus 0 = 0$ $\quad 0 \oplus 1 = 1$ $\quad 1 \oplus 0 = 1$ $\quad 1 \oplus 1 = 0$).

Cette relation peut être réécrite autrement, à savoir que le résultat de la mesure de C est entièrement conditionné par les résultats des mesures de A et de B. De fait, quels que soient x_B et x_C on a toujours :

$$x_A = x_B \oplus x_C .$$

On peut interpréter ce résultat en disant que les mesures préalables de x_B et de x_C prédéterminent celle de x_A. Cela n'est en soi pas plus étrange que le fait que dans l'expérience à deux particules intriquées, la mesure du spin de l'une conditionne celle de l'autre. Seule l'expression de la loi de conservation a changé.

Une théorie à variables cachées locales se trouve à nouveau embarrassée pour expliquer la prédisposition qu'a le qubit A de révéler systématiquement la valeur $x_A = x_B \oplus x_C$ alors que le système se trouvait initialement dans un état $|\psi\rangle$ parfaitement symétrique pour toute permutation des symboles A, B et C. Einstein y aurait encore vu une preuve que la description initiale, en terme de $|\psi\rangle$, est incomplète et qu'il y a lieu d'y ajouter un élément supplémentaire de réalité étranger à la théorie quantique et capable de prendre en compte la prédisposition du qubit A. Cette idée ne tient pas la route pour la raison suivante. Modifions le protocole expérimental et raisonnons par l'absurde. On commence par soumettre chacun des qubits, B et C, à une porte de Hadamard avant de procéder aux mesures des trois qubits. Le système modifié se trouve donc, juste avant ces mesures, dans l'état :

$$H_C H_B |\psi\rangle = Z_2 X_1 |\psi\rangle .$$

S'il existait un élément de réalité locale capable de prédisposer la mesure de A, on ne voit pas ce que le fait d'imposer une porte de Hadamard à B et C pourrait changer à cela : les trois qubits peuvent être aussi éloignés que l'on veut et ils n'interagissent pas.

La présence des portes de Hadamard modifient la relation qui relie les résultats des mesures. On a maintenant dans tous les cas :

$$x_A \oplus x_B^H \oplus x_C^H = 1 .$$

Ces résultats demeurent si on permute les indices A, B et C, en sorte que l'on peut encore écrire :

$$x_A^H \oplus x_B \oplus x_C^H = 1 \qquad \text{et} \qquad x_A^H \oplus x_B^H \oplus x_C = 1 .$$

Il est maintenant facile de voir qu'on aboutit à une contradiction, il suffit de sommer (modulo 2) les quatre conditions précédentes pour obtenir :

$$(x_A \oplus x_B \oplus x_C) \oplus (x_A \oplus x_B^H \oplus x_C^H) \oplus (x_A^H \oplus x_B \oplus x_C^H) \oplus (x_A^H \oplus x_B^H \oplus x_C) = 1$$

or le membre de gauche devrait valoir 0 car l'ordre des termes y est indifférent et que chaque symbole y apparaît deux fois. La conclusion est que les prémices étaient fausses et qu'il n'y a pas d'élément de réalité supplémentaire à incorporer à la théorie quantique.