Transcription d'un texte de Yannis Delmas-Rigoutsos [1] au sujet de la logique quantique

IV. Synthèse : la logique quantique

§ 1. Définition : la logique de la mécanique quantique

Cette logique a été introduite comme telle par von Neumann et Birkhoff [16]. C'est au départ la logique de la mécanique quantique, c'est à dire la logique sous-tendant les faits expérimentaux de la mécanique quantique.

Dans la formalisation de la mécanique quantique donnée par von Neumann l'état physique du système étudié (pour nous de l'Univers) est représenté par un vecteur dans un espace de Hilbert, lequel représente tous les possibles. Les quantités mesurables sont appelée observables et le fait de pratiquer une mesure d'une observable O revient à projeter le vecteur sur un sous-espace de notre espace de Hilbert, lequel sous-espace détermine une valeur mesurée o pour O (ou, en général, une gamme G de valeurs).

Par des méthodes que nous ne détaillerons pas, on peut voir que l'assertion "telle mesure de O donnerait une valeur dans une certaine gamme G" pour un système préparé d'une certaine façon correspond à un sous-espace de l'espace de Hilbert choisi pour modéliser les possibles. De plus, modulo des postulats adéquats, tout tel sous-espace correspond à une mesure (ou combinaison de mesures) réalisable en théorie.

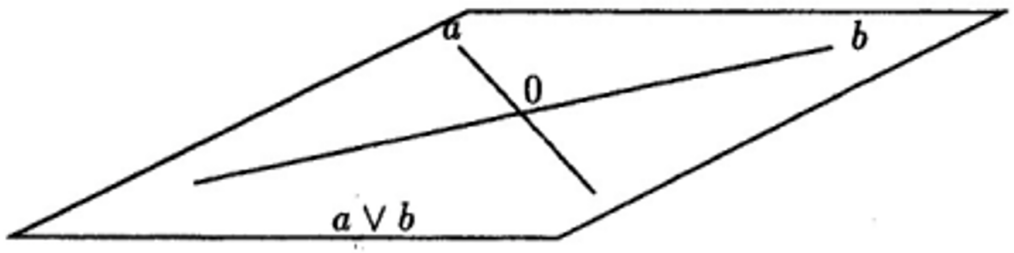
Plus généralement, la logique quantique (abstraite) est la logique dont les propositions sont les sous-espaces d'un espace de Hilbert donné. La conjonction (le "et") est l'intersection de deux sous-espaces, leur disjonction ("ou") est la somme fermée de deux sous-espaces, et la négation d'un sous-espace est son orthogonal. Il nous faut maintenant détailler tout ceci pour qui ne serait pas familier de ces notions.

§ 2. De nouveaux diagrammes de Venn

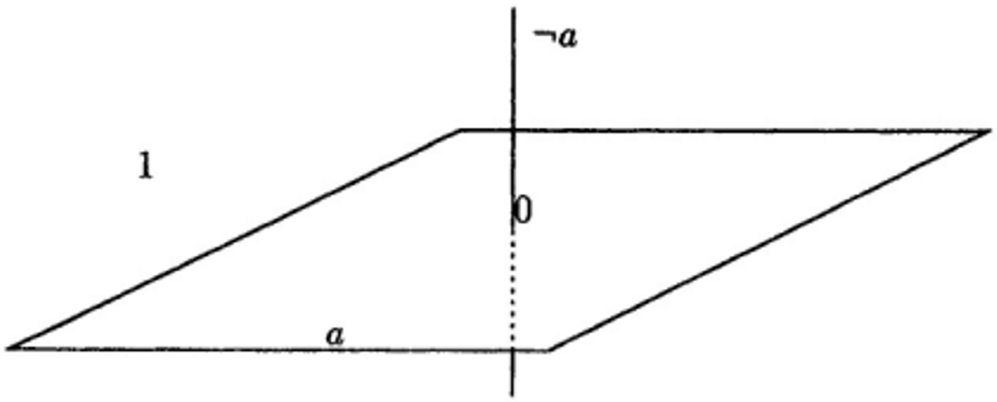
Tout comme la logique classique était la logique des ensembles, la logique quantique est la logique des espaces de Hilbert. Un espace de Hilbert de dimension finie peut être vu comme l'espace euclidien habituel de même dimension (à la différence qu'en général, les coordonnées sont des nombres complexes). Ses sous-espaces sont les espaces de Hilbert plus petits que (inclus dans) lui. Notons que comme nous parlons d'espaces vectoriels, tous ces espaces contiennent 0, qui représente le "faux".

Ainsi, si a et b sont deux droites, leur disjonction, $a \vee b$ sera un plan :

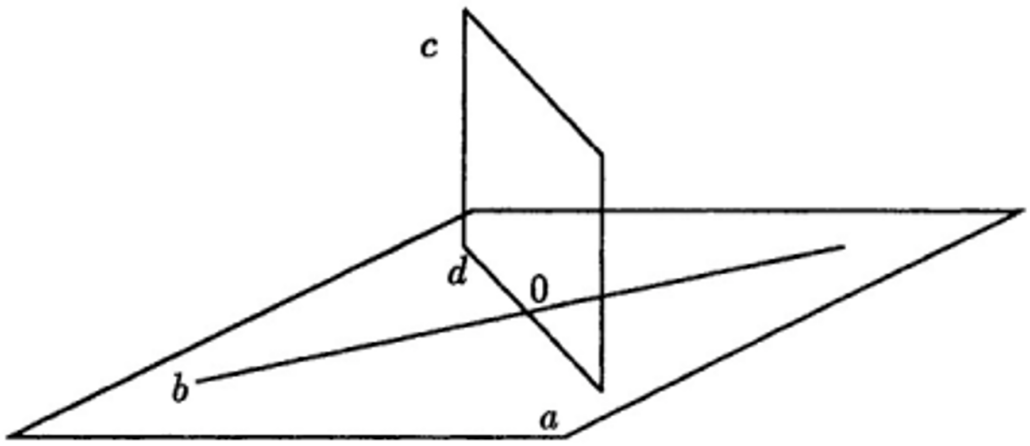
[1] Référence : Yannis Delmas-Rigoutsos, Logique quantique, Séminaire de Philosophie et Mathématiques, fascicule 5, "Logique quantique", p. 1-23, 1993. Voir http://www.numdam.org/article/SPHM_1993___5_A1_0.pdf. Transcription en Latex : Denise Vella-Chemla, janvier 2025.



Si notre espace de Hilbert de référence (représentant le "vrai", que nous notons 1) est "notre" espace à 3 dimensions, et si a est un plan, $\neg a$ ("non a") sera la droite orthogonale à a (passant par 0) :



Dans la figure suivante, nous avons $b \leq a$ et $d = a \,\&\, c$, par exemple. $b \leq a$ signifie en termes d'espaces que b est inclus dans a, et en termes logiques que b implique a. De même, $d = a \,\&\, c$, signifie en termes d'espaces que d est l'intersection de a et c et en termes logiques que d est équivalent à "a et c".



En fait la notion complète est un peu plus complexe que cela du fait que certaines figures doivent être réalisées en dimension 4, 5, ou même, quand il s'agit de la mécanique quantique, en dimension infinie. Cependant, avec un peu d'imagination, on peut se rendre compte que ces schémas (en

dimension quelconque) vont jouer le même rôle que les diagrammes de Venn en logique classique. Avant de voir cela, il faut donner une définition axiomatique de la logique quantique en définissant les connecteurs par des règles, comme on peut le faire pour la logique classique. Ceci est plus opératoire, même si moins intuitif a priori.

Notons, pour terminer, que ces diagrammes peuvent et doivent servir d'intuition pour la logique quantique. En effet, il est tentant, quand on dispose d'un formalisme, d'essayer de saisir le "sens" des connecteurs ; malheureusement, comme on s'en doute, l'expérience montre que tout est possible en matière de sémantique. Dans le cas de la logique quantique, on trouve ceux qui affirment que le sens des connecteurs est le même qu'en logique classique et que seules changent des choses plus complexes comme la distributivité. Mais il y a aussi ceux qui disent que & et $\vee$ changent mais pas $\neg$, ceux qui pensent que c'est $\neg$ mais pas & et $\vee$ et ceux qui pensent que c'est $\vee$ mais pas & et $\neg$,... Nous ne nous lancerons pas dans une polémique si intéressante. Nous nous contenterons de dire qu'une possibilité est de visualiser le & comme en logique classique, le $\vee$ comme englobant une idée de positions logiques intermédiaires, enfin le $\neg$ comme UNE négation, en retenant cependant que celle-ci n'est pas unique. Ce n'est cependant pas le seul moyen : on peut, par exemple, centrer son interprétation sur la relation de compatibilité.

§ 3. **La notion de compatibilité**

Pour obtenir une logique utilisable de manière courante, il n'est pas possible de se ramener systématiquement à la mécanique quantique ou aux espaces de Hilbert : il lui faut une description et un fondement autonome. Il sera toujours possible, ensuite, de recourir à une interprétation fournie par la mécanique quantique.

Avant toute chose, il faut définir ce qu'est une formule de la logique quantique. Ce point est facile : les formules de la logique quantique sont les mêmes que celles de la logique classique, seul leur "sens" diffère. Si les lettres a, b,... représentent des formules de la logique quantique, on veut donner un sens à $a \leq b, 0, 1, \neg, a \vee b, a \,\&\, b$ et $a \to b$. Pour cela on ajoute la relation $a \frown b$ et on pose les axiomes suivants [2] :

1. $\leq$ est une relation d'ordre, c'est à dire que $a \leq b \leq c$ implique $a \leq c$, et $a \leq b \leq a$ équivaut à $a = b$ ($a \leq b$ correspond à la relation "a implique b" et $a = b$ à "a équivaut à b"),
2. 0 et 1 sont respectivement le plus petit et le plus grand élément ("faux" implique tout et "vrai" est impliqué par tout),
3. $a \vee b$ est le plus petit élément supérieur à a et b,
4. $a \,\&\, b$ est le grand élément inférieur à a et b,
5. $\neg a \vee a = 1$ (tiers exclu) et $a \,\&\, \neg a = 0$ (non-contradiction),
6. par définition $a \to b$ vaut $\neg a \vee (a \,\&\, b)$ ($a \to b$ est une formule qu'il faut bien distinguer de la relation $a \leq b$),

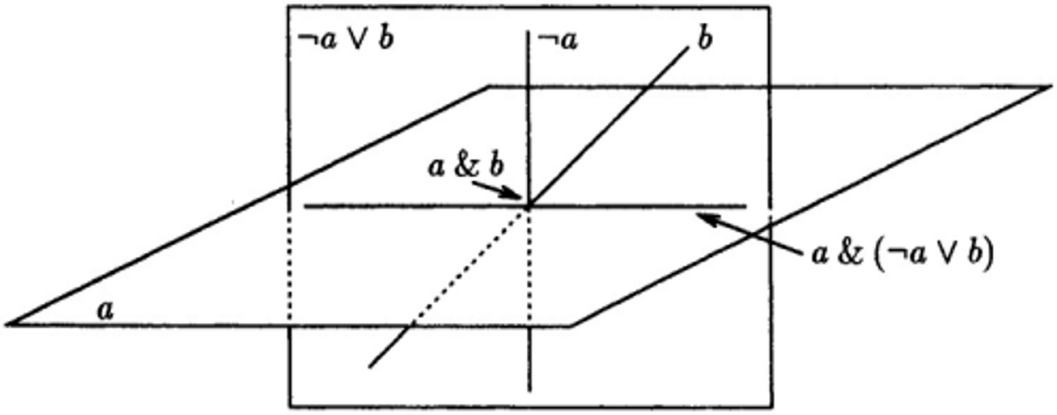
[2] On peut aussi présenter ces axiomes sous forme de règles de déduction, comme on le fait pour un certain nombre de logiques. On peut voir en appendice la présentation de P. Gibbins [5].

7. on dit que a et b sont **compatibles**, et on note $a \frown b$, si $a \,\&\, b = a \,\&\, (\neg a \vee b)$, on impose que si $a \leq b$ alors $a \frown b$.

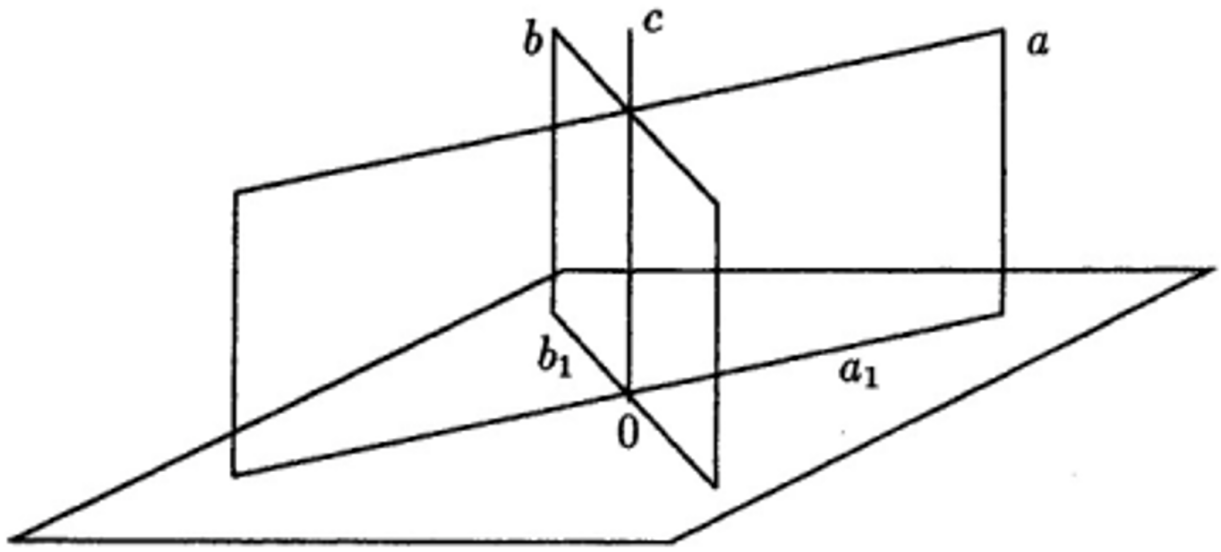
En fait tous les axiomes sauf le dernier correspondent à ce que l'on pourrait poser en logique classique, à part peut-être l'implication qui se définit plus simplement par $\neg a \vee b$ (mais cette expression est équivalente à l'autre en logique classique). La différence vient de ce qu'en logique classique, deux éléments quelconques satisfont toujours cette relation un peu étrange :

$$a \,\&\, b = a \,\&\, (\neg a \vee b).$$

Ce n'est pas le cas en logique quantique. Comme on le voit sur la figure ci-dessous, deux propositions quelconques ne sont pas nécessairement compatibles (cette figure est une figure en 4 dimensions dont l'une a été "écrasée") :



En fait, avec nos pseudo-diagrammes de Venn, $a \,\&\, (\neg a \vee b)$ est la projection de b sur a ; ainsi a et b sont compatibles si la projection de l'un sur l'autre est l'intersection des deux. Cette relation est symétrique mais pas transitive. On peut également démontrer en logique quantique que la compatibilité équivaut à se décomposer en espaces orthogonaux : $a \frown b$ si et seulement si $a = a_1 \vee c, b = b_1 \vee c$ où a_1, b_1 et c sont deux-à-deux orthogonaux :



Une autre manière équivalente de voir ceci est de dire que a et b satisfont une relation de distributivité, par exemple

$$a \,\&\, (b \vee \neg b) = (a \,\&\, b) \vee (a \,\&\, \neg b).$$

On peut même démontrer que si parmi $a, \neg a, b, \neg b$, une relation de distributivité non-évidente (ne découlant pas des premiers axiomes) est vraie alors a et b sont compatibles.

Physiquement deux propositions seront compatibles si les mesures correspondantes peuvent être réalisées simultanément. De manière générale, sont compatibles deux éléments d'une vision cohérente de la réalité.

§ 4. **La notion de négation**

Un autre moyen de voir la différence qui peut exister entre logique classique et logique quantique est de considérer cette dernière comme construite sur la première, à la différence près de l'existence de plusieurs négations.

Cette manière de voir assez riche peut se conforter à notre intuition. En effet, on peut classiquement supposer que "non-X" est la propriété de tout ce qui n'est pas X ; dans la pratique se pose alors le problème, dans certains cas, de délimiter "X" précisément, tout ce qui ne rentre pas dans ce cadre étant étiqueté non-X. Or, si l'on se rappelle le cas des paradoxes dits *sorites* (de $\sigma\omega\rho\acute{o}\zeta$, "tas"), on voit que ceci n'est pas clair du tout. Ainsi, si l'on s'intéresse au passage de l'état de têtard à celui de crapaud (paradoxe de Cargile), et que l'on pose X ="être un crapaud", il n'est pas clair que le non-X le plus intéressant soit défini par "ne pas être un crapaud" mais bien plutôt par "être un têtard". Même si pour l'essentiel ces deux définitions sont équivalentes, elles expriment dans le détail des points de vue très différents.

Ceci est un défaut de la négation classique, et on aimerait bien, de fait, une négation plus proche de ce qu'on pourrait appeler la négation linguistique des substantifs. Ne connaissant que le domaine

indo-européen, nous nous restreindrons à celui-ci, bien que le pendant soit très certainement vrai pour d'autres familles linguistiques. En indo-européen, donc, nous avons un préfixe privatif dont l'idée va plus loin qu'une simple négation classique. Cette négation du nom apparaît de manière fortement non classique en grec (préfixe $\alpha\nu$-) et en sanskrit (préfixe *an*-). On pensera au mot anarchie qui nous vient du grec ou a l'idée de *non-violence* qui a eu un certain bonheur en Inde. Ainsi l'"an-arch-ie" n'est pas simplement le fait qu'il n'y ait pas de gouvernement mais va plus loin, se réfère à une certaine *négation* de la notion d'état (négation justement, mais dans le sens habituel, pas logique). De même, être "non-violent", n'est pas le simple fait de ne pas être "violent", mais d'adhérer à une théorie qui rejette la "violence", "sous toutes ses formes". Ainsi la négation du substantif, au moins dans ces langues, et au moins pour un certain nombre de cas, ne doit pas être visualisée par la négation au sens classique, mais par la *negatio* latine [3], voire même souvent par une opposition.

Si nous prenons l'exemple des couleurs, que nous admettrons disposées selon le "cercle chromatique" (une sphère serait plus exacte), on peut considérer que "rouge" correspond à telle plage de fréquences (à la nuance près du problème de frontière que nous avons soulevé). Mais que va-t-on poser comme "non-rouge" ? On peut prendre, conformément à la logique classique, "tout ce qui n'est pas rouge", mais cela nous amènera certainement à prendre comme "non-rouge" des choses imperceptiblement différentes du "rouge". Dans l'optique de la logique quantique, il peut être intéressant de prendre pour "non-rouge" la signification "vert" (Fig. 1, ci-contre). L'important est de noter que, dans cette optique, plusieurs possibilités s'offrent à nous ; nous avons choisi "vert" qui correspond à la décomposition physiologique (rouge/vert, jaune/bleu) ou à la décomposition classique rouge/jaune/bleu, mais nous aurions pu choisir "cyan" qui correspond à la décomposition télévisuelle rouge/vert/bleu (Fig. 2), ou encore "bleu" qui correspond à une décomposition chaud/froid... Une infinité de possibilités se présentent qui peuvent être plus ou moins adaptées à tel ou tel problème.

Bien entendu, dans cette optique quantique, le $\vee$ ne correspond plus à l'intuition classique : il s'agit maintenant plutôt d'interpréter $a \vee b$ comme "a, b, ou tout ce qu'on peut avoir comme propriétés intermédiaires".

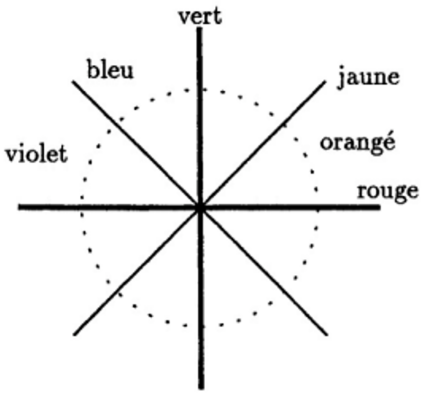


FIG. 1

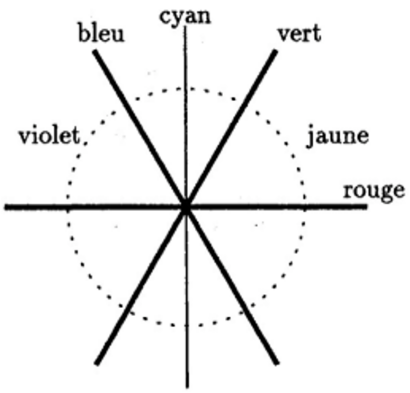


FIG. 2

[3]On peut voir replacée dans un cadre plus général l'opposition qui existe en latin entre *aio* et *nego* : cf. Benveniste, [1], livre 3, chapitre 6, *Le vocabulaire latin des signes et présages.*

§ 5. **Les probabilités quantiques**

Nous avons vu qu'un système de propositions qui satisfait les axiomes ci-dessus peut se représenter comme une collection de sous-espaces d'un espace de Hilbert, soit un équivalent des diagrammes de Venn. Or ceux-ci permettent de saisir l'intuition d'une probabilité classique. Nous en voudrions un équivalent quantique.

Ceci est possible dans une certaine mesure. Voyons-le en dimension finie. Dans un diagramme de Venn, l'aire d'une zone est intuitivement le nombre de points ou de surfaces élémentaires qu'elle contient (si la surface du dessin est quadrillée par exemple). Dans les espaces de Hilbert, les plus petits sous-espaces non-nuls qui puissent intervenir sont les droites (les points de la géométrie projective correspondante). On ne peut, bien sûr, pas prendre comme mesure le nombre de droites puisque, ne serait-ce que dans un plan, ce nombre est infini. Par contre, on peut prendre le nombre de droites compatibles contenues dans cet espace. Ce nombre est exactement la dimension de celui-ci puisque deux droites compatibles sont orthogonales [4].

Dans un espace de Hilbert de dimension finie la probabilité d'une proposition peut donc être définie comme le rapport de la dimension du sous-espace associé par celle de l'espace total. Pour ceux qui connaissent, on peut dire également que si π est le projecteur associé ou sous-espace, cette dimension est $\mathrm{Tr}(\pi)$ et donc, si ρ_0 est l'opérateur de densité associé au système, la probabilité désirée est $\mathrm{Tr}(\rho_0\pi)$, formule connue.

Dans un espace de Hilbert de dimension infinie, tout n'est pas perdu, car nous avons la notion d'observable et, une observable étant donnée, on peut lui associer une intégrale correspondant à une probabilité sur l'espace des mesures possibles de cette observable. On peut également prendre dans la même optique l'opérateur de densité. Ceci définit une probabilité conforme à l'intuition que nous avons donnée sur les sous-espaces compatibles avec cette observable (et qui correspondent donc aux gammes de valeurs mesurables de cette observable) ; par contre, pour les autres sous-espaces, l'interprétation (et même la définition) se fait moins naturellement.

§ 6. **Application à la mécanique quantique**

a. Introduction : une justification du formalisme

La première application que l'on aurait souhaité pour la logique quantique à la mécanique quantique est une résolution simple et satisfaisante des "paradoxes" qu'elle entraîne. Nous verrons ce point plus loin : il n'est pas évident. Par contre, un usage immédiat peut être fait qui est celui de la justification du formalisme. Quand on observe le formalisme de la mécanique quantique, il y a matière à s'interroger : pourquoi des espaces de Hilbert ? Pourquoi les probabilités quantiques ? En somme, pourquoi un outil aussi malcommode à comprendre ? La logique quantique peut apporter une réponse partielle à ces questions.

Le fait physique irréductible à toute explication est l'existence de ce qu'on appelle le quantum

[4] Techniquement, pour assurer que ceci soit possible il faut rajouter quelques suppositions physiquement justifiables. Voir Piron [13] : démonstration et détails.

d'action qui fait que quand deux sous-systèmes de l'Univers (par exemple l'expérimentateur et le système étudié) interagissent, il existe une quantité minimale d'interaction. La conséquence immédiate de ceci est qu'il arrive une limite au-delà de laquelle les interactions ne peuvent plus être négligées. En particulier, les mesures perturberont toujours les systèmes étudiés et ceci d'autant plus qu'elles seront plus précises. La conséquence en est, incidemment, que la position au cours du temps, par exemple, ne peut décrire complètement un système puisqu'elle correspond à une chose mesurable plus qu'à une réalité intrinsèque. Ici intervient la notion d'observables incompatibles : **un système complet d'observables comporte nécessairement des observables incompatibles**.

Une logique de la réalité prenant en compte ces faits jouira donc des caractéristiques suivantes :

- on veut avoir une conjonction, une disjonction, et une négation qui se comportent vis-à-vis de la relation d'implication comme dans le cas classique,
- on *doit avoir* une notion de compatibilité telle que si des propositions sont deux-à-deux compatibles, elles se comportent comme dans le cas classique,
- *il existe* des propositions incompatibles.

Ceci étant posé, la logique quantique est le modèle logique le plus simple qui remplisse ces conditions. Nous avons vu qu'alors un modèle naturel est la collection des sous-espaces d'un espace de Hilbert muni, comme observables des opérateurs (hilbertiens) sur cet espace, et comme négation, de l'orthogonalité. Nous avons vu que ce que l'on appelle en général les probabilités quantiques peuvent être supposées également à la suite.

Pour ce qui est enfin du rapport expérimental, des mesures d'observables, on peut encore arriver à le justifier mais la démarche est plus indirecte. En effet, une observable, même si on suppose qu'elle correspond à une propriété de l'Univers, reste rapportée à un instrument de mesure. À l'aide d'hypothèses raisonnables sur ce rapport, on peut retrouver l'essentiel de la formulation traditionnelle de la mécanique quantique.

Pour avoir en fait TOUTE la formulation traditionnelle, il resterait le problème du temps, que nous avons éludé. Ceci est certainement particulièrement épineux, et il n'est pas clair du tout que les formulations actuelles soient même très satisfaisantes sur ce point...

b. Les variables cachées

Un autre point lié au formalisme se discute aussi particulièrement bien à la lumière de la logique quantique, celui des variables cachées. À ce sujet, une confusion est très généralement entretenue : il ne s'agit pas de savoir s'il existe des variables cachées sous-tendant la mécanique quantique ou si celle-ci décrit vraiment la réalité physique ; ce savoir nous est inaccessible. Il s'agit de savoir s'il existe des variables cachées CLASSIQUES et si la mécanique quantique est complète DANS LE SENS QUE NOUS AVONS INDIQUÉ PLUS HAUT et à nos limites expérimentales près.

Ceci étant posé, on se convainc assez facilement que si un système admet une description classique, par exemple au moyen de variables cachées, alors ceci revient à considérer que les propositions

quantiques qui nous intéressent sont des propositions particulières d'un système classique. En termes mathématiques, cela revient à plonger notre système quantique de propositions dans une algèbre de Boole en respectant la négation et l'implication. Or on peut démontrer assez facilement que si le système de propositions engendré par deux propositions quantiques a et b se plonge (de cette manière) dans une algèbre de Boole, alors a et b sont compatibles et c'est une algèbre de Boole.

Ainsi on peut démontrer que **si les principes logiques énoncés plus haut sont satisfaits, alors il ne peut y avoir de variables cachées classiques sous-tendant le système physique**. Et ceci se démontre par un simple examen logique : il n'est pas nécessaire de rentrer dans les complications du formalisme.

Références

[1] E. Benveniste, *Vocabulaire des institutions indo-européennes. II : pouvoir, droit, religion.*, collection *Le sens commun*, Editions de Minuit, 1969.

[5] P. Gibbins, A user-friendly quantum logic, *Logique et Analyse* 112 (1985), pages 353-362.

[13] C. Piron, Axiomatique quantique, *Helvetica Physica Acta* 37 (1964), pages 439-468

[16] J. von Neumann, G. Birkhoff, The logic of quantum mechanics, *Annals of Mathematics* 37 (1936), pages 823-843.

Traduction du paragraphe 2 du texte arxiv https://arxiv.org/pdf/quant-ph/9708050

2. Les principes du calcul quantique

Les principes du calcul quantique ont été présentés en détail ailleurs (voir par exemple [8, 17]) donc nous n'en donnerons ici qu'une brève introduction. L'idée essentielle du calcul quantique est de représenter des nombres binaires en utilisant une collection de systèmes quantiques à deux niveaux. On utilisera la notation $\{|0\rangle, |1\rangle\}$ pour dénoter les états d'un système unique à deux niveaux, appelé bit quantique ou *qubit*.

Avec plusieurs qubits, le nombre de degrés de liberté du système augmente rapidement : l'espace de Hilbert décrivant l'état d'un système contenant N qubits a 2^N dimensions. Il est possible d'utiliser un tel système pour représenter un nombre, x, entre 0 et $\left(2^N - 1\right)$, comme l'état

$$|x\rangle \equiv \prod_{i=0}^{N-1} |x_i\rangle_i, \tag{1}$$

où $x = \sum_{i=0}^{N-1} x_i 2^i$, et x_i est le $i^{\text{ième}}$ chiffre binaire de x. Ainsi, par exemple, le nombre décimal qui s'écrit 1011 en binaire, serait représenté par 4 qubits dans l'état $|1\rangle_3|0\rangle_2|1\rangle_1|1\rangle_0$, ce qu'il est plus pratique d'écrire en notation abrégée $|1011\rangle$.

Pour effectuer des calculs, on a besoin d'effectuer certaines opérations unitaires qui agissent sur un ensemble de qubits, appelées *portes logiques quantiques*. Comme les interactions quantiques sont réversibles, la logique sous-jacente à un ordinateur quantique doit elle-même être réversible. Heureusement, on sait déjà que les opérations booléennes arbitraires peuvent être construites de façon réversible [18], [19].

Voyons l'exemple de l'opération logique réversible NON sur un seul qubit :

$$\text{NON} : |b\rangle \rightarrow |\bar{b}\rangle. \tag{2}$$

Les opérations arithmétiques nécessitent d'effectuer des opérations logiques entre deux ou plusieurs qubits. Par exemple, dans l'opération NON contrôlée sur deux qubits

$$\text{CNOT} : |c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle,$$

un qubit cible, t, voit sa valeur changée lorsqu'un qubit de contrôle, c, a la valeur 1, mais reste inchangé lorsque le qubit de contrôle a la valeur 0. Le symbole $\oplus$ dénote l'addition modulo 2, définie par la table de vérité suivante :

a	b	a $\oplus$ b
0	0	0
0	1	1
1	0	1
1	1	0

.

Une seconde application de la porte CNOT ramène l'état à sa valeur initiale.

Une autre porte logique réversible en calcul quantique est le NON contrôlé par 3 bits (ou porte de Toffoli) :

$$\text{CCNOT} : |c_1\rangle|c_2\rangle|t\rangle \rightarrow |c_1\rangle|c_2\rangle|\,(c_1 \wedge c_2) \oplus t\rangle, \tag{3}$$

où $\wedge$ dénote le ET logique défini par la table de vérité :

a	b	a $\wedge$ b
0	0	0
0	1	0
1	0	0
1	1	1

.

En utilisant des portes de Toffoli et des portes CNOT, on peut construire un additionneur binaire simple :

$$\text{ADD}\,(|a\rangle, |b\rangle, |0\rangle) = \text{CNOT}_{1,2}\,(\text{CCNOT}\,(|a\rangle, |b\rangle, |0\rangle)) = |a\rangle|a \oplus b\rangle|a \wedge b\rangle \tag{4}$$

qui place la somme modulo 2 de la première et de la seconde entrées (en lisant de gauche à droite) sur la seconde sortie, et la retenir (qui se lit initialement 0) sur le troisième qubit en sortie. (Ici, l'opération CNOT sur trois qubits est définie comme : $\text{CNOT}_{1,2} : |a\rangle|b\rangle|c\rangle \rightarrow |a\rangle|a \oplus b\rangle|c\rangle$).

Avec ces portes logiques quantiques *universelles*, on peut former des fonctions arithmétiques arbitraires.

Jusque-là, notre discussion n'a révélé aucun pouvoir particulier, qui serait associé au calcul quantique. En effet, il est clair que la nécessité physique de la réversibilité logique amène une extra-information (par rapport au calcul conventionnel) qui est reportée. Cette extra-information, qui permet de déterminer l'entrée d'une opération logique à partir de la sortie, impose des contraintes de mémoire additionnelles sur le calcul quantique. Néanmoins, on sait que les concepts quantiques de superposition et d'interférence, en particulier, peuvent être utilisés pour fournir une solution beaucoup plus efficace pour certains problèmes, que ne le permettent les ordinateurs conventionnels. Considérons d'abord les calculs avec superpositions de nombres. Une opération unitaire sur un seul qubit peut s'écrire :

$$(k, \phi) : \left\{ \begin{array}{l} |0\rangle \\ |1\rangle \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \cos\left(\frac{k\pi}{2}\right)|0\rangle - i\exp\left(i\phi\right)\sin\left(\frac{k\pi}{2}\right)|1\rangle \\ \cos\left(\frac{k\pi}{2}\right)|1\rangle - i\exp\left(-i\phi\right)\sin\left(\frac{k\pi}{2}\right)|0\rangle \end{array} \right\}. \tag{5}$$

Par exemple, $(1/2, \pi/2) : |0\rangle \rightarrow 2^{-1/2}\,(|0\rangle + |1\rangle)$, est une superposition également pondérée de deux états de qubits. Maintenant, commencer avec un registre L-qubit dans l'état $|0\rangle \equiv \prod_{i=0}^{L-1} |0\rangle_i$ et agir

sur chacun des qubits avec $(1/2, \pi/2)$ produit une superposition cohérente de tous les 2^L nombres possibles :

$$|0\rangle \to 2^{-L/2} \prod_{i=0}^{L-1} (|0\rangle_i + |1\rangle_i) = 2^{-L/2} \sum_{a=0}^{2^L-1} |a\rangle. \tag{6}$$

Ainsi, dans un certain sens, la mémoire d'un ordinateur quantique est exponentiellement grande. Maintenant, l'état du registre quantique ci-dessus est un état produit, alors qu'un état de superposition plus typique du registre sera un état intriqué (i.e. un état qui ne peut pas s'écrire comme un simple produit tensoriel d'états de base). De tels états peuvent être produits à l'aide des opérations quantiques logiques. Par exemple, un état intriqué de deux qubits peut être produit à partir d'un état produit initial :

$$\text{CNOT} : 2^{-1/2} (|0\rangle + |1\rangle) |0\rangle \to 2^{-1/2} (|0\rangle|0\rangle + |1\rangle|1\rangle) . \tag{7}$$

Les états intriqués sont nécessaires durant les calculs quantiques typiques (et c'est l'existence de telles intrications qui distingue un ordinateur quantique d'un ordinateur classique), mais à cause de leurs propriétés non classiques, l'opération CNOT est extrêmement difficile à construire dans un système physique.

Jusque là, nous avons vu la puissance de la mémoire quantique. Explorons maintenant la puissance des calculs quantiques effectifs. Supposons que nous ayons déterminé la séquence de portes quantiques nécessaires pour évaluer (de manière réversible) la valeur d'une certaine fonction, F, pour une donnée quelconque, a :

$$\widehat{F} : |a\rangle|0\rangle \to |a\rangle|F(a)\rangle, \tag{8}$$

où l'argument est maintenu dans le registre de gauche, et où le registre de droite conserve la valeur de la fonction. On aurait pu tout aussi bien commencer avec le registre de gauche dans une superposition également-pondérée de toutes les valeurs, et appliquer la même séquence de portes logiques :

$$\widehat{F} : \sum_{a=0}^{2^L-1} |a\rangle|0\rangle \to \sum_{a=0}^{2^L-1} |a\rangle|F(a)\rangle, \tag{9}$$

en évaluant toutes les 2^L valeurs de la fonction en une seule étape. (Rappelons que l'état intial du registre de gauche peut être créé à partir de l'état $|0\rangle$ avec des opérations unitaires à qubit L-unique). Si l'on n'est intéressé que par les valeurs de la fonction, on doit répéter la création de cet état $O(2^L)$ fois, et mesurer le registre droit à chaque fois pour déterminer les valeurs. De façon évidente, pour ce type de problème, le calcul quantique n'offre aucun avantage, mais si l'on est intéressé par une propriété commune partagée par toutes les valeurs de fonction, comme la période de la fonction, on pourrait maintenant effectuer une opération de transformation de Fourier quantique (QFT) sur le registre de gauche pour déterminer efficacement la période. Le point clé est que les valeurs de

cette fonction particulière dans le registre de droite sont associées aux séquences de valeurs dans le registre de gauche qui reflètent la période. La QFT, qui est donnée par la formule suivante

$$|a\rangle \rightarrow 2^{-\frac{L}{2}} \sum_{c=0}^{2^L-1} \exp\left(i\frac{a.c}{2^L}\right)|c\rangle, \tag{10}$$

regroupe ces séquences pour produire une interférence constructive aux valeurs correspondant aux périodes de la séquence. De plus, la QFT elle-même peut être construite en utilisant seulement $O(L^2)$ portes quantiques, alors que la transformation de Fourier discrète conventionnelle nécessite $O(L2^L)$ opérations pour un registre L-bits en entrée. Pour les problèmes qui peuvent se réduire à déterminer la période d'une fonction, le calcul quantique peut offrir une solution plus efficace que le calcul conventionnel. Tous les algorithmes quantiques connus pour résoudre des problèmes intéressants utilisent plutôt la QFT ou bien l'une de ses variantes, comme la transformation de Hadamard.

Références

[8] A. Ekert, R. Jozsa, Rev. Mod. Phys. 68 (1996) 733-753.

[17] S. Lloyd, Scientific American (October 1995) 140-145.

[18] C. H. Bennet, IBM J. Res. Dev. 6 (1979) 525.

[19] E. Fredkin, T. Toffoli, Int J. Theor. Phys. 21 (1982) 219-253.