

Logique et mécanique quantique : ceci explique cela ?

Marc Bagnol et Anne-Sophie de Suzzoni,
sous la direction de Thierry Paul

Septembre 2009

Référent LMFI : Pierre-Louis Curien

Table des matières

1	Introduction	5
2	Guide de lecture	8
3	Rudiments de logique linéaire	10
4	Les espaces cohérents	13
4.1	La polarité	13
4.2	Espaces cohérents probabilistes	14
5	Mécanique Quantique	16
5.1	Principes	16
5.1.1	Espaces de Hilbert, états quantiques	16
5.1.2	Notations	16
5.1.3	Observables et mesure	17
5.1.4	Couplage et produit tensoriel	18
5.1.5	Notions de trace partielle et d'opérateur de densité	18
5.1.6	Reformulation des principes en termes d'opérateurs de densité	19
5.1.7	Transformations admissibles, superopérateurs	19
5.1.8	Principe de non-clonage	20
5.2	Intrication	20
5.2.1	Critère d'Horodecki	21
5.2.2	Transposition et intrication	22
5.3	Exemples	24
5.3.1	Spin n , symétries	24
5.3.2	Symétries et dimension	24
5.3.3	Observable de spin total	25
5.3.4	Produit tensoriel de deux spins	25
6	Du classique au quantique (en quittant la diagonale)	27
7	Propriétés des ECQ	29
7.1	Polarité et géométrie : le théorème du Bipolaire	29
7.2	Applications linéaires et produit tensoriel	30
7.3	Connecteurs	32
7.3.1	Additifs	32
7.3.2	Multiplicatifs	33
7.3.3	Distributivité	33
7.3.4	Éléments neutres	34
8	Un exemple-clé : les booléens quantiques	36
8.1	Par et intrication	36
8.2	Valeurs propres négatives dans les ECQ	42
8.3	Retour sur les cas classiques et probabilistes	44
9	Un exemple qui se généralise	47
9.1	Espaces de Hilbert-Schmidt	47
9.2	Normes L^p	49

10 Autour de la positivité	52
10.1 De l'isomorphisme à la dualité	52
10.2 L'isomorphisme de Selinger	53
10.2.1 Superpositivité	54
10.3 Ce qui change avec les ECQ, conséquences	55
10.4 Réconcilier les deux approches ?	55
11 Espaces Cohérents Positifs	58
11.1 Le théorème du Bipolaire	58
11.2 L'isomorphisme dans le cas positif	60
11.3 Les connecteurs positifs	61
11.3.1 Additifs	61
11.3.2 Multiplicatifs	62
11.3.3 Distributivité	62
11.4 Booléens et connecteurs	63
11.5 Positivité et dimension infinie	65
11.6 Un autre exemple : l'électron et le positron	65
11.6.1 Espaces cohérents positifs et projections	65
11.6.2 Equation de Dirac	67
11.6.3 Lien avec les espaces cohérents positifs	68
12 Interprétation des preuves	69
12.1 η en logique	70
12.2 η dans les ECQ	71
13 Conclusion	72
A Annexe	74
A.1 Les règles de la logique linéaire	74
A.2 Modélisation des algorithmes quantiques avec contrôle classique et diminution de la trace	76
A.2.1 Boucles quantiques	76
A.2.2 Cas d'une boucle qui ne termine pas	78
B Bibliographie	80



1 Introduction

Un peu d'histoire...

Alors que le début du XX^{ème} siècle a vu la logique émerger comme un domaine des mathématiques à part entière, le fin de ce même siècle a été le théâtre de profonds changements dans la façon d'aborder le sujet.

Après quelques interrogations sur la théorie des ensembles, la première grande question de la logique sera le programme lancé par Hilbert en 1900. Les interrogations portaient sur les fondements des mathématiques, on peut les résumer en deux points :

- La question de la cohérence des mathématiques : le système formel que l'on utilise peut-il mener à une contradiction ?
- La question de la complétude : peut-on toujours démontrer ou réfuter un énoncé mathématique ?

C'est Gödel qui apportera la réponse en 1931 avec ses célèbres théorèmes d'incomplétude : tout système formel suffisamment expressif pour encoder l'arithmétique ne peut être à la fois cohérent et complet.

Le résultat a mis un certain temps à être bien compris, et les recherches autour du programme de Hilbert se sont poursuivies avec plus ou moins de succès pendant plusieurs décennies.

Ainsi, en 1934 Gentzen va mettre sur pied la déduction naturelle, puis le calcul des séquents, pour obtenir un cadre plus pratique pour raisonner sur les démonstrations. Initialement conçu pour démontrer la cohérence de l'arithmétique au moyen d'une induction ordinale (une généralisation de la récurrence), le calcul des séquents sera le point de départ de la transformation de la logique à la fin du XX^{ème} siècle.

En effet, pour faire sa démonstration, Gentzen montre un résultat intermédiaire sur le calcul des séquents : l'élimination des coupures.

L'idée est que la coupure correspond *grosso modo* à l'utilisation de lemmes intermédiaires. Il existe un algorithme dit *d'élimination des coupures* qui transforme une démonstration en une autre, démontrant la même chose sans utiliser la coupure.

Cet algorithme constitue la première apparition d'un point de vue dynamique en logique.

Bien que la terminaison de l'algorithme d'élimination des coupures implique la cohérence, on peut être tenté d'aller un peu plus loin. Les propriétés d'un algorithme à étudier ne manquent pas : le temps qu'il met à terminer, dans quelles situations termine-t'il rapidement, peut-on optimiser le calcul, quel est l'espace nécessaire pour effectuer le calcul etc.

À cela va s'ajouter une remarque de Curry¹ : il existe une correspondance forte entre les preuves (de logique intuitionniste en particulier) et la notion de programme informatique, par l'intermédiaire du λ -calcul. Par exemple, le programme qui prend en argument un élément de type A et le retourne sans modification correspond à une preuve de $A \Rightarrow A$.

Dans cette correspondance, c'est justement l'élimination des coupures qui joue le rôle de l'exécution du programme.

À partir de là, la question en logique va progressivement glisser de « *est-ce que A est vrai ?* » vers « *comment A est vrai ?* » avec l'informatique à la fois comme source d'inspiration et champ d'application.

¹Curry avait remarqué cette correspondance pour la logique combinatoire, mais c'est un article de Howard dans le cadre du λ -calcul simplement typé qui a fait connaître l'idée. C'est pourquoi on parle généralement de la "correspondance de Curry-Howard".

La logique linéaire

C'est dans ce contexte qu'apparaît la logique linéaire. Issue d'une analyse de la dynamique de la logique, elle propose un changement de point de vue : les formules deviennent des sortes de ressources, sur lesquelles on effectue des actions. Ce qui donne une vision presque "physique" de la logique.

Ainsi, on ne lit plus « $A \Rightarrow B$ » comme « *si A est vrai, B est vrai* », mais plutôt comme « *on peut transformer A en B* ». On change d'ailleurs de notation pour bien marquer la différence : l'implication linéaire se note « $A \multimap B$ ».

En particulier, la duplication d'hypothèses s'apparente à une duplication de ressources et nécessite un traitement particulier.

Le nom de la logique *linéaire* n'est pas un hasard. Il vient d'une propriété ensembliste sur des fonctions qui fait fortement penser à la "vraie" linéarité. Il est donc assez naturel de chercher à faire vivre la logique linéaire dans des espaces vectoriels. Or, les objets quantiques se décrivent justement à l'aide d'espaces de Hilbert.

De plus, cette idée d'une implication qui *consomme, détruit* sa prémisse fait penser à ce qui se passe en mécanique quantique, où se produisent des phénomènes du type *principe de non-clonage*. On va donc chercher à interpréter la logique linéaire dans un monde quantique, afin de voir ce que peut apporter le passage d'une vision de la logique comme actions à une vision comme actions quantiques.

L'information quantique

La vision d'action quantique, ou de transformation décrite de façon ponctuelle sur des systèmes quantiques prend son sens en information quantique. On retrouve l'idée d'action à travers la notion de porte quantique, analogues des portes logiques en informatique. L'évolution temporelle des systèmes est en effet "cachée" dans le passage de ces portes.

Plus précisément, on considère des objets quantiques, des chaînes de Qubits, auxquels on applique des transformations linéaires. Le passage d'une porte quantique est l'application sur une chaîne de Qubits d'une transformation linéaire de base. On fera correspondre ces transformations à des preuves de logique linéaire.

En pratique, un Qubit peut revêtir plusieurs formes. C'est en tout cas un système quantique à deux niveaux d'énergie, notés $|0\rangle$ et $|1\rangle$, comme un bit classique peut avoir deux valeurs, 0 et 1. Faire passer une porte à une chaîne de Qubits correspond à faire évoluer son état pendant un temps donné. Cette évolution est linéaire, et avant et après le passage d'une porte, l'état du registre de calcul est considéré comme stable.

On peut pour cela utiliser des photons. Un Qubit est alors un ensemble de deux cavités optiques. L'état $|0\rangle$ correspond à l'événement "le photon est dans la première cavité", l'état $|1\rangle$ à "le photon est dans la deuxième cavité". On agit sur le système en utilisant des miroirs, et des miroirs semi-réfléchissants.

On peut également utiliser des pièges à ions. Le Qubit est dans ce cas un noyau atomique dont l'état $|0\rangle$ est le niveau d'énergie fondamental et $|1\rangle$ le niveau d'énergie excité à 1 phonon, c'est-à-dire son mode de vibration le plus bas. On agit sur son état à l'aide d'impulsions laser, et les Qubits sont couplés par le partage d'un phonon.

Enfin, un Qubit peut être le spin d'un noyau nucléaire, que l'on fait évoluer en modifiant le champ électro-magnétique (de fortes impulsions magnétiques) dans lequel le noyau est plongé.

Un des défis majeurs de l'information quantique est de réussir à stabiliser suffisamment longtemps une chaîne de Qubits. Un de ses intérêts est la possibilité de réduire des problèmes dont la complexité optimale connue est exponentielle en des problèmes de complexité polynomiale (factorisation des grands nombres, algorithme de Shor, transformée de Fourier).

Cependant, ce gain en complexité va de pair avec une perte d'assurance sur le résultat. En effet, la mécanique quantique est intrinsèquement probabiliste, si bien que le résultat d'un algorithme quantique est le résultat voulu à une certaine probabilité près. On a donc besoin de contrôler classiquement ces résultats.

Dans cette optique, en 2003, P. Selinger construit une sémantique de l'algorithmique quantique : il donne une représentation de chaque algorithme quantique à travers des opérateurs positifs dans lesquels il intègre le contrôle classique, ce qui lui permet en particulier de représenter les boucles ou les procédures récursives.

On a ici une sorte d'assimilation entre les objets de l'information quantique, les Qubits (représentés également par des opérateurs positifs), et les transformations (linéaires, donc) que l'on opère sur eux. P. Selinger rend cette assimilation possible à travers un isomorphisme entre les applications superpositives (transformations admises par la mécanique quantique) et les opérateurs positifs.

J.-Y. Girard s'en est inspiré en 2004 pour définir la version quantique de ses espaces cohérents : les espaces cohérents quantiques, qui sont un modèle d'une partie de la logique linéaire. L'isomorphisme qu'il utilise est différent et n'impose aucun contrôle sur la positivité des opérateurs, ce qui amènera quelques problèmes. En particulier, l'identité des opérateurs, qui est la représentation de la preuve de l'axiome $A \multimap A$ se transforme *via* l'adjonction en un opérateur non positif. J-Y Girard est donc obligé d'admettre dans son modèle des opérateurs non-positifs, mais aussi en conséquence des applications qui ne sont pas superpositives, donc qui ne sont pas admises par la mécanique quantique et n'ont pas d'analogues en algorithmique.

Néanmoins, les espaces cohérents quantiques présentent énormément d'analogies avec l'information quantique, notamment à travers l'utilisation du produit tensoriel. On retrouve également une interprétation du phénomène de décohérence.

2 Guide de lecture

Nous nous sommes dans un premier temps intéressés de près au modèle des espaces cohérents quantiques introduit par J.-Y. Girard dans [8]. Nous en avons d'abord étudié les aspects techniques, puis nous nous sommes penchés sur un exemple peu détaillé dans l'article : les booléens quantiques, censés correspondre à un ensemble d'états quantiques. Ceci nous a permis de point de départ pour les remarques sur la positivité et la superpositivité évoquées ci-dessus. Nous nous sommes également intéressés à l'interprétation de l' η -expansion dans ce modèle, qui donne des résultats très différents des modèles classiques.

La fin du mémoire est consacrée à la construction d'un modèle alternatif, s'inspirant à la fois des espaces cohérents quantiques et du modèle construit dans [15] par P. Selinger, dont on utilisera l'isomorphisme. Les résultats les plus intéressants sur ce modèle étant que l'on peut alors se restreindre aux opérateurs positifs et aux transformations superpositives, et que le \mathfrak{K} de systèmes quantiques correspond alors exactement à la combinaison libre des deux sous-systèmes, intrication comprise.

Détail du contenu de chaque section :

Dans les sections 3 et 4, on introduira la logique linéaire d'un point de vue très intuitif, pour les non-logiciens. On verra ensuite rapidement quelques notions sur les espaces cohérents classiques et probabilistes afin de comprendre leur lien de parenté avec les espaces cohérents quantiques.

On exposera ensuite (section 5) les notions de mécanique quantique utilisées dans ce mémoire : principes de base, transformations superpositives, intrication.

Dans les sections 6 et 7, on posera les définitions de base des espaces cohérents quantiques, puis on en étudiera des propriétés plus avancées.

Les sections suivantes seront consacrées à l'étude de plusieurs exemples. Le plus important d'entre eux étant celui des booléens quantiques (section 8), qu'on comparera avec leurs analogues classique et probabiliste.

On regardera également des généralisations de cet exemple (section 9.2).

Cela nous permettra de mettre en lumière une divergence entre les espaces cohérents quantiques et la mécanique quantique. On s'intéressera dans la section 10 à cette divergence, en comparant le modèle (et surtout son adjonction) de J.-Y. Girard et celui de P. Selinger.

Cela nous mènera à proposer une construction alternative, combinant les idées à la base des espaces cohérents quantiques et de la sémantique de P. Selinger. On étudiera en section 11 les propriétés de cette construction qui permet de ne garder que des opérateurs positifs.

Enfin, on verra (section 12) une partie de l'interprétation des preuves de la logique linéaire dans les espaces cohérents quantiques. Cette interprétation a la particularité de faire la différence entre une preuve et sa version η -expansée, fait assez inhabituel en logique. De plus, on remarquera que le passage de l'une à l'autre version se fait par "mesure sans lecture".

Note : Insistons sur le fait qu'à notre connaissance, la relecture de l'article de Selinger à la lumière des espaces cohérents quantiques n'avait pas produit auparavant la construction d'espaces cohérents dont les éléments sont exclusivement des opérateurs positifs. De surcroît, les exemples que nous avons développés sont issus d'une remarque de J.-Y. Girard concernant la structure des ECQ canoniques que lui-même a construit : plutôt que de les voir comme le bipolaire d'un ensemble, il choisit de les considérer comme un ensemble d'opérateurs positifs associé à une norme. Ce point de vue n'avait, d'après nos lectures, pas encore été exploité et nous a permis de former des espaces cohérents à la fois quantiques et positifs. Enfin, nous avons mis en exergue les relations entre booléens classiques, probabilistes et quantiques.

3 Rudiments de logique linéaire

Une logique de ressources

Un bon moyen de comprendre le sens de l'implication linéaire est d'y penser en termes économiques : « $A \multimap B$ » prend le sens de « *il faut payer A pour obtenir B* ». Contrairement à une implication classique, dans une démonstration de $A \multimap B$ on part de l'hypothèse A mais on ne peut l'utiliser *qu'une seule fois* pour démontrer B (tout comme une pièce de 50 centimes ne peut servir que pour acheter un seul café au distributeur).

La logique linéaire ne se contente pas d'une implication. Outre les connecteurs que nous détaillerons un peu plus bas, on dispose d'une **négation**, notée “ \sim ”.

Là où la négation usuelle inverse les valeurs de vérité, la négation linéaire prend un sens plus opérationnel. Si A est une ressource, on peut voir $\sim A$ comme une *demande* de A , une sorte d'anti- A , tel que A et $\sim A$ mis en présence l'un de l'autre se détruisent mutuellement. On retrouve en logique linéaire le principe « $A \multimap B$ si et seulement si $\sim B \multimap \sim A$ », mais son sens a changé : on est face à un *renversement* du processus de transformation de A en B .

Mais tout cela resterait assez exotique (quoiqu'intéressant) si la logique linéaire n'avait aucun lien avec les logiques dont elle est censée expliciter l'opérationnalité. L'idée est qu'une modalité, notée “ $!$ ” va redonner aux énoncés un comportement classique.

Pour continuer sur la métaphore économique, posséder $!A$ c'est être très riche ! En effet l'interprétation intuitive de $!A$ est « *A autant que l'on veut, ad libitum* ».

Cela permet de faire le lien avec la logique usuelle via l'équation suivante :

$$A \Rightarrow B \simeq !A \multimap B$$

qui dit que démontrer que A implique B est équivalent à démontrer *linéairement* B en utilisant un nombre potentiellement infini de fois A .

Les connecteurs

Puisque l'on considère les énoncés comme des ressources, on ne peut plus les manipuler de la même façon que des valeurs de vérité.

On sent bien qu'il va y avoir beaucoup plus de manières différentes de “mettre ensemble” deux ressources que de combiner deux tables de vérité. Le système étant plus fin, son langage est plus complexe.

Cela se traduit entre autres par un doublement du nombre de connecteurs, dont on peut essayer de donner une intuition en continuant à suivre la métaphore économie/ressources :

Le « tenseur », \otimes

C'est le connecteur le plus simple à comprendre : $A \otimes B$ peut se lire « *j'ai A et B simultanément* ». En particulier $A \otimes A$ se traduit en « *deux fois A* », ce que le “et” logique habituel ne peut pas exprimer, puisque “ A ” à la même table de vérité que “ $A \text{ et } A$ ”.

Le « avec », $\&$

La proposition $A \& B$ se lit « *A ou B , au choix* ». Cela se comprend bien avec la règle suivante² : si $A \multimap B$ et $A \multimap C$, alors $A \multimap B \& C$, qui se traduit en « *si à partir de A je peux avoir B et à partir de A je peux avoir C , alors à partir de A je peux avoir B et C (mais pas les deux !)* »

Ces deux connecteurs se comportent plutôt comme un “et” dans le système de preuve de la logique linéaire, mais font apparaître son ambiguïté quand on l'utilise pour parler de ressources.

²Le système complet des règles de la logique linéaire est disponible en [annexe](#).

Le « plus », \oplus

$A \oplus B$ se lit « A ou B , sans avoir le choix ». Là encore on peut l'illustrer par une règle : si $A \rightarrow C$ et $B \rightarrow C$, alors $A \oplus B \rightarrow C$. La dernière implication “attend” un A ou un B , sans savoir lequel des deux sera fourni, pour le transformer en C .

Le « par », \wp

Le connecteur \wp est le plus difficile à décrire. Son rapport avec l'implication linéaire va un peu nous aider : en réalité, l'implication linéaire n'est pas un connecteur “primitif”. On le définit justement à l'aide du \wp , en posant $A \rightarrow B := \sim A \wp B$. Vu sous cet angle, on peut écrire que $A \wp B = \sim A \rightarrow B = \sim B \rightarrow A$, c'est à dire un système composé de A et de B qui attend un anti- A ou un anti- B pour interagir avec et renvoyer B ou A selon le cas.

\oplus et \wp sont deux formes de “ou” si l'on considère les règles qui leur sont associées dans le système logique, mais sont très différents du point de vue opérationnel.

Le menu et la solution

Pour illustrer cette introduction, faisons marcher ces intuitions sur deux exemples. On va décrire avec le langage de la logique linéaire des situations mettant en jeu des transformations.

Le menu :

Un restaurant japonais propose le menu suivant :

Menu B4 , 11 € :

- Sushis de thon ou de saumon (selon le marché)
- Bière ou thé vert
- Riz à volonté

On peut décrire ce menu dans le langage de la logique linéaire de la façon suivante :

$$(11\text{€}) \rightarrow (\text{Thon} \oplus \text{Saumon}) \otimes (\text{Bière} \& \text{Thé}) \otimes !\text{Riz}$$

Le restaurant est donc vu comme un moyen de transformer 11€ en un menu, qui contient à la fois (connecteur \otimes) un plat, une boisson et du riz ; le plat présentant un choix *qui n'est pas fait par le client* (connecteur \oplus), au contraire de la boisson (connecteur $\&$) et le riz est à *volonté* (modalité !).

La solution :

Lors d'une expérience de chimie, on dispose d'une solution contenant une mole de A et une mole de B , et dans un récipient différent d'une mole d'un produit $\sim A$ qui précipite en présence de A . De plus, on sait qu'une mole de B change de couleur en présence d'une mole de C pour devenir B' , altérant la mole de C au passage, qui devient une mole de C' .

(précisons que le système qui nous intéresse est bien la solution et les composés dissous, en particulier tout ce qui est solide et déposé au fond du récipient —par exemple le résultat d'une précipitation— est considéré comme “hors du système”)

La solution correspond à un *par* : $A \wp B$. Le fait que A et $\sim A$ précipitent se traduit par

$$(A \wp B) \otimes \sim A \rightarrow B$$

et le changement de couleur de B par $B \otimes C \rightarrow B' \wp C'$. En mettant tout ensemble on obtient :

$$(A \wp B) \otimes \sim A \otimes C \rightarrow B' \wp C'$$

qui décrit l'expérience en cours.

Cet exemple illustre bien l'idée évoquée plus haut pour le connecteur \wp : on a à disposition les deux solutés, mais *mélangés* dans le même récipient. C'est toute la différence avec $A \otimes B$ qui serait A et B dans deux récipients *séparés*. Ainsi on peut lire la formule $X \otimes Y \rightarrow X \wp Y$ comme « *mélanger une mole de A et une mole de B donne une solution de A et B* »³.

Avec le \wp , on doit faire un choix : pour récupérer uniquement du B , il faut faire précipiter A avec une mole de $\sim A$.

³Pour les logiciens : on est face à une interprétation "chimique" de la règle du *Mix*.

4 Les espaces cohérents

On va introduire dans cette section les espaces cohérents sous une forme qui nous permettra de passer naturellement à leur version quantifiée.

4.1 La polarité

Les espaces cohérents sont nés de l'étude de la sémantique du λ -calcul.⁴

Sans entrer dans les détails, l'idée est de construire une interprétation des preuves (de la logique intuitionniste au départ, puis de la logique linéaire) afin de mieux comprendre leur fonctionnement. Ainsi, à chaque formule A , on associe un espace cohérent $[A]$ contenant des éléments qui vont correspondre à des "preuves partielles"⁵ de A en logique linéaire, identifiant au passage les preuves équivalentes (au sens de l'élimination des coupures).

Par exemple, l'espace cohérent $[\sim A]$ est formé d'éléments correspondant à des "preuves partielles" de $\sim A$, l'espace cohérent $[A \otimes B]$ est formé d'éléments correspondant à "une preuve partielle de A et une preuve partielle de B mises ensemble".

Dans les espaces cohérents la décomposition

$$A \Rightarrow B \simeq !A \multimap B$$

dont on a parlé plus haut apparaît naturellement.

La définition initiale des espaces cohérents manipule des graphes et des sous-graphes connexes (appelés cliques) de ces graphes. Il existe une définition alternative en termes de *polarité* :

Définition : polarité

Soit $|A|$ un ensemble quelconque (qu'on appellera *trame*). On dit que deux parties x et y de $|A|$ sont polaires si

$$\#|x \cap y| \leq 1, \text{ ce qu'on notera } x \perp y$$

Si A est un ensemble de parties de $|A|$, on pourra parler du *polaire* de A :

$$\sim A := \{ b \mid \forall a \in A, b \perp a \}$$

Remarque : pour comprendre d'où vient cette définition, il faut regarder une autre façon d'écrire la négation linéaire : $\sim A \simeq A \multimap \perp$, que l'on interprète par l'ensemble des fonctions (linéaires) de A dans \perp , l'espace cohérent à un seul élément. Tout élément "y" du polaire de A définit une telle fonction en associant l'ensemble vide ou le singleton contenant l'unique élément de \perp à tout x dans A selon que x et "y" ont un élément commun ou non.

Définition : espace cohérent

Un espace cohérent (EC) de trame $|A|$ est un sous-ensemble A de $\mathcal{P}(|A|)$ qui est égal à son bipolaire, i.e., tel que $A = \sim \sim A$.

Remarque : en logique linéaire, la négation retrouve son statut involutif, tout comme $\neg \neg A = A$ en logique classique (mais pas en logique intuitionniste), on a $\sim \sim A = A$. Évidemment, cette propriété

⁴Dans les années 60, D. Scott avait construit le premier exemple de catégorie cartésienne fermée différent de la catégorie des ensembles, les *domaines de Scott*. Les espaces cohérents sont au départ une simplification due à J.-Y. Girard des domaines de Scott, lesquels peuvent devenir assez rapidement illisibles si on essaie de faire marcher les définitions concrètement. Cette simplification est due à la notion de stabilité, dont l'emploi a été suggéré par une vision plutôt catégorique, alors que l'intuition des domaines Scott est plutôt topologique.

⁵Si on ne prenait que de "vraies" preuves, quand A est prouvable on devrait avoir $[non-A]$ vide, et le modèle ne pourrait pas fonctionner.

prend un sens très différent ici, puisqu'elle dit essentiellement qu'un "anti-anti-A" est la même chose que A.

C'est pour cette raison que l'on demande aux espaces cohérents, qui interprètent la logique linéaire, d'être égaux à leur bipolaire.

L'intérêt de cette présentation par rapport à la version "graphes" est qu'elle est plus *interactive* et nécessite moins de notions ensemblistes, elle va ainsi pouvoir s'exporter plus facilement. On peut illustrer cette remarque en reformulant, au moins pour le cas fini, ces notions en termes de matrices et de traces. Cela constituera un premier pas vers le monde quantique, où il est plutôt question d'espaces vectoriels et de matrices que d'ensembles et de graphes.

Définition : matrice représentant un sous-ensemble

Si $|A| = \{a_1, a_2, \dots, a_n\}$ est une trame (finie) et $x \subseteq |A|$ on associe à x la matrice diagonale M_x suivante :

$$\begin{pmatrix} \varepsilon_1 & & & \\ & \varepsilon_2 & & \\ & & \ddots & \\ & & & \varepsilon_n \end{pmatrix} \text{ où } \varepsilon_i \text{ vaut } 1 \text{ si } a_i \in x \text{ et vaut } 0 \text{ sinon.}$$

On a alors les propriétés :

- Le cardinal de x est égal à la trace de M_x .
- L'intersection de x et y correspond à la matrice $M_{x \cap y} = M_x M_y$

La conséquence de ceci est qu'on peut exprimer la polarité sans faire appel aux notions de cardinalité et d'intersection :

Définition alternative de la polarité :

$$x \perp y \text{ si et seulement si } Tr(M_x M_y) \leq 1 .$$

Exemple : sur une trame $|A|$, l'ensemble $B_{|A|}$ des singletons de A est un espace cohérent.

En effet, $\sim B_{|A|}$ contient **tous** les sous-ensembles de $|A|$. Et le polaire de $\sim B_{|A|}$ est exactement l'ensemble des singletons. Cet exemple est détaillé en 8.3.

Cette vision matricielle des espaces cohérents et de la polarité va nous permettre d'introduire une notion de probabilité, qui est une première forme d'indétermination, pas encore quantique.

4.2 Espaces cohérents probabilistes

L'idée des espaces cohérents probabilistes est de remplacer les sous-ensembles de la trame par des lois de probabilités.

Ce point de vue se représente également très bien en termes de matrices :

Définition : matrice représentant un sous-ensemble probabiliste

Si $|A| = \{a_1, a_2, \dots, a_n\}$ est une trame (finie) et x un sous-ensemble "probabiliste" (décrit par la probabilité que $a_i \in x$) de $|A|$, on associe la matrice diagonale M_x suivante :

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix} \text{ où } \lambda_i \text{ vaut } p(a_i \in x) .$$

La trace de M_x devient alors l'espérance du cardinal de x et celle de $M_x M_y$ l'espérance du cardinal de " $x \cap y$ ". On définit la polarité de la même façon que précédemment :

Définition : polarité des espaces cohérents probabilistes

$x \perp y$ si et seulement si $Tr(M_x M_y) \leq 1$.

On peut définir ainsi les espaces cohérents probabilistes.

Définition : espace cohérent probabiliste

Un espace cohérent probabiliste (ECP) de trame $|A|$ est un sous-ensemble probabiliste A de $|A|$ qui est égal à son bipolaire.

Exemple : sur une trame $|A|$ donnée, l'ensemble $B_{|A|}$ des sous-ensembles probabilistes dont le cardinal a une espérance inférieure ou égale à 1 est un ECP. En termes matriciels, il s'agit simplement des matrices diagonales à coefficients dans $[0, 1]$ et de trace inférieure ou égale à 1. Cet exemple est également détaillé en [8.3](#).

5 Mécanique Quantique

Plutôt que de décrire le fonctionnement de la mécanique quantique, nous définirons ici les objets qu'elle met en jeu, les espaces cohérents ne permettant pas d'adopter un point de vue dynamique. Ainsi, les notions d'évolution temporelle et donc d'équation de Schrödinger ne seront pas traitées. En revanche, ils décrivent des processus. En ce sens, on se retrouve assez proche de l'information quantique.

Nous parlerons en revanche d'intrication, de spin, et de transformations sur les états, qui sont des notions indispensables en information quantique. De plus, nous évoquerons certains isomorphismes sur des espaces de spins susceptibles d'admettre un analogue en logique linéaire, dans le cadre des espaces cohérents.

5.1 Principes

5.1.1 Espaces de Hilbert, états quantiques

Revenons tout d'abord à la mécanique classique. L'état d'un système, par exemple un point matériel, est décrit par la donnée de deux grandeurs mesurables : la position q et l'impulsion p . Ces données peuvent avoir différentes valeurs dans un cadre général mais l'état d'un système fixe cette valeur.

En mécanique quantique, on parle de superposition d'états. Si un système S peut être dans un état e_1 ou un état e_2 alors l'état $\alpha e_1 + \beta e_2$ existe et décrit la possibilité, mais ne s'y réduit pas, d'être dans l'état e_1 avec probabilité $|\alpha|^2$ ou dans l'état e_2 avec probabilité $|\beta|^2$. En mécanique classique, on n'imagine pas un électron se trouvant à différentes positions à la fois.

Donnons un exemple. L'électron a pour spin $\frac{1}{2}$. C'est-à-dire qu'en plus de son moment cinétique "classique" (le fait qu'il tourne autour d'un proton par exemple), il dispose d'un moment cinétique intrinsèque (le spin) qui peut valoir $\frac{1}{2}$ ou $-\frac{1}{2}$. L'électron peut donc se trouver dans l'état "spin = $\frac{1}{2}$ " noté $|+\rangle$, ou "spin = $-\frac{1}{2}$ ", noté $|-\rangle$. La mécanique quantique nous dit qu'il peut également se trouver dans un état $\frac{1}{\sqrt{2}}|+\rangle + \frac{i}{\sqrt{2}}|-\rangle$.

Ce principe, appelé *principe de superposition*, requiert que les états d'un système soient décrits par des vecteurs. C'est pourquoi on utilise des espaces vectoriels, et plus précisément des espaces de Hilbert.

L'état d'un système est donc la donnée d'un espace de Hilbert H et d'un vecteur de norme égale à 1, la norme considérée étant celle associée au produit scalaire hermitien.

Dans le cas du spin $\frac{1}{2}$, on a $H = \text{Vect}(|+\rangle, |-\rangle)$.

Remarque : l'état d'un système est défini à une phase globale près, c'est-à-dire que si $|\psi\rangle$ décrit un état E et que θ est un réel, l'état décrit par $e^{i\theta}|\psi\rangle$ est également E . Ceci apparaîtra plus clairement lors de la discussion sur la notion de mesure.

5.1.2 Notations

- On note $|\phi\rangle$ les vecteurs de H , où ϕ est "l'étiquette" de l'état.
- Le produit scalaire hermitien de deux vecteurs $|\psi\rangle, |\phi\rangle$ est noté $\langle\psi|\phi\rangle$. Par convention, il est linéaire à droite (et donc antilinéaire à gauche).
- La forme linéaire sur $H : |\psi\rangle \mapsto \langle\phi|\psi\rangle$ est notée $\langle\phi|$.

De cette façon, on peut mettre toutes les applications linéaires sous la forme d'une somme de $|\phi\rangle\langle\psi|$. En particulier, la projection sur la droite $\mathbb{C}|\psi\rangle$ s'écrit $|\psi\rangle\langle\psi|$. (Avec $|\psi\rangle$ de norme 1.)

Donnons quelques exemples d'opérateurs pour le spin $\frac{1}{2}$, avec leurs représentations matricielle dans la base $|+\rangle, |-\rangle$.

La projection $|-\rangle\langle-|$ a pour matrice :

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

L'opérateur $|+\rangle\langle -|$, qui, à $|-\rangle$, associe $|+\rangle$, est représenté par la matrice :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

L'opérateur de Hadamard H est défini par $H|+\rangle := \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ et $H|-\rangle := \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$, s'écrit :

$$H = \frac{1}{\sqrt{2}} \left(|+\rangle\langle +| + |+\rangle\langle -| + |-\rangle\langle +| - |-\rangle\langle -| \right)$$

et a pour matrice :

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

Cet opérateur appartient à la base universelle des opérateurs servant à décrire toutes les portes quantiques. Utilisé avec une porte control-NOT, il sert à créer de l'intrication.

Le control-NOT (ou CNOT) est l'opérateur agissant sur deux spins $H \otimes H$ tel que le deuxième électron passe de $|+\rangle$ à $|-\rangle$ et vice versa si et seulement si le premier est dans l'état $|+\rangle$. Autrement dit,

$$\text{CNOT : } \begin{aligned} |+, +\rangle &\mapsto |+, -\rangle \\ |+, -\rangle &\mapsto |+, +\rangle \\ |-, +\rangle &\mapsto |-, +\rangle \\ |-, -\rangle &\mapsto |-, -\rangle \end{aligned}$$

ce qui se représente par la matrice :

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

5.1.3 Observables et mesure

On veut pouvoir modéliser le processus de mesure sur un système, par exemple, connaître le spin d'un électron. Rappelons que si l'électron est dans l'état $\alpha|+\rangle + \beta|-\rangle$, son spin est $+\frac{1}{2}$ avec probabilité $|\alpha|^2$ ou $-\frac{1}{2}$ avec probabilité $|\beta|^2$.

Le processus de mesure revient à projeter l'état de l'électron sur $|+\rangle$ ou $|-\rangle$ en fonction du résultat de la mesure, en renormalisant (car tous les vecteurs d'état ont pour norme 1).

Soit

$$S := \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

écrite dans la base $(|+\rangle, |-\rangle)$. Cette matrice a pour valeurs propres $\frac{1}{2}$ et $-\frac{1}{2}$ et pour vecteurs propres $|+\rangle$ et $|-\rangle$.

Mesurer le spin d'un électron revient donc à projeter l'état de l'électron sur un sous-espace propre de la matrice et la valeur obtenue est la valeur propre associée à cet espace. S est la matrice (on parle d'observable) associée au spin.

Plus généralement, on appelle observable tout opérateur autoadjoint O de H . Ces opérateurs sont orthogonalement diagonalisables et ont des valeurs propres réelles. Chaque grandeur mesurable du système correspond à une observable. Les mesures possibles sont les valeurs propres de O .

Supposons que l'on dispose d'un système dans l'état $|\psi\rangle$ et que O admette pour valeur propre λ associée au projecteur orthogonal P_λ , la probabilité que la mesure de O donne λ est $p_\lambda = \langle \psi | P_\lambda | \psi \rangle$. Si P_λ se met sous la forme $|\psi_\lambda\rangle\langle \psi_\lambda|$, on a $p_\lambda = |\langle \psi_\lambda | \psi \rangle|^2$.

La mesure agit alors ainsi sur le système : après mesure, l'état du système est donné par $\frac{P_\lambda |\psi\rangle}{\sqrt{P_\lambda}}$. Remarquons que la mesure est un processus fondamentalement non linéaire.

Par ailleurs, l'indépendance vis-à-vis de la phase globale s'explique ici. En effet, ce qui nous intéresse dans les états quantiques est leur interaction avec l'expérimentateur *via* la mesure. Or, p_λ est indépendant de la phase globale de l'état. Autrement dit, si deux vecteurs sont colinéaires, leur interaction avec le système de mesure est la même. L'expérimentateur "voit" la même chose, les états décrits sont indifférentiables.

5.1.4 Couplage et produit tensoriel

Nous avons un électron, supposons qu'à présent nous disposons également d'un photon, de spin 1. Le spin du photon peut valoir -1 , 0 , ou 1 , états décrit respectivement par $|-1\rangle$, $|0\rangle$, et $|1\rangle$. Ce nouveau système (à deux particules donc) requiert un nouvel espace de Hilbert.

Voyons quels sont les éléments de base qui décrivent l'état du système. On désigne par e ce qui est relatif à l'électron, et par p au photon. On dispose des états décrits par $|e : -, p : -1\rangle$, $|e : -, p : 0\rangle$, $|e : -, p : 1\rangle$, $|e : +, p : -1\rangle$, $|e : +, p : 0\rangle$, et $|e : +, p : 1\rangle$. Ces vecteurs forment une base pour le nouvel espace de Hilbert. Cet espace est le produit tensoriel de l'espace relatif à l'électron et de celui relatif au photon : $H = H_e \otimes H_p$, avec $|e : a, p : b\rangle = |a\rangle \otimes |b\rangle$.

Dans le cas général, si un système S_1 est décrit par H_1 et un système S_2 est décrit par H_2 , alors l'état du système $S = S_1 \cup S_2$ est décrit par les vecteurs de $H_1 \otimes H_2$.

Il y a deux types de vecteurs dans cet espace : les vecteurs dits séparables, qui peuvent se mettre sous la forme $|\phi\rangle \otimes |\psi\rangle$, et les autres dits intriqués. Remarquons qu'à partir d'un état séparable, décrit par un vecteur $|\chi\rangle = |\phi\rangle \otimes |\psi\rangle$, on peut retrouver toute l'information sur l'état d'un sous-système. En effet, pour tout opérateur A de H_2 , on a $\langle \chi | (Id \otimes A) | \chi \rangle = \langle \psi | A | \psi \rangle$. On peut donc retrouver $|\psi\rangle$ à partir de $|\chi\rangle$ à une phase globale près.

L'intrication, ou l'existence d'états intriqués, revêt une importance fondamentale en mécanique quantique. En effet, deux systèmes intriqués ne peuvent évoluer indépendamment l'un de l'autre, et ce même s'ils sont séparés spatialement, c'est-à-dire s'ils ne sont plus couplés par des interactions fondamentales car à trop grande distance l'un de l'autre. C'est de là que sont nées les théories de l'information et de la cryptographie quantique.

5.1.5 Notions de trace partielle et d'opérateur de densité

A présent, nous pouvons faire une remarque quant à l'état de l'électron. Ce dernier ne vit pas seul, il est couplé à son environnement. Le système à considérer n'est donc pas simplement l'électron seul, mais l'électron évoluant dans son environnement. Autrement dit, l'état du système est décrit par un vecteur $|\chi\rangle$ du produit tensoriel $H_{env} \otimes H_e$, où H_{env} est l'espace de Hilbert relatif à l'environnement.

Cependant, c'est à l'électron que l'on s'intéresse et non à la partie compliquée de $|\chi\rangle$ appartenant à H_{env} . L'information que l'on obtient est donnée par les mesures que l'on peut effectuer. Soit $O \in \mathcal{L}(H_e)$ une observable pour l'électron. L'opérateur $I \otimes O$ admet les mêmes valeurs propres que O . Et, si $|v\rangle$ est un vecteur propre de O , alors $|*\rangle \otimes |v\rangle$ est un vecteur propre de $I \otimes O$. L'observable $I \otimes O$ est donc liée à la mesure de O . On voudrait avoir un vecteur $|\psi\rangle$ tel que $\langle \psi | O | \psi \rangle = \langle \chi | Id \otimes O | \chi \rangle$ quelle que soit l'observable O . Malheureusement, dans le cas général, un tel vecteur n'existe pas. En revanche, il existe une matrice ρ vérifiant $Tr(O\rho) = Tr((I \otimes O)|\chi\rangle\langle\chi|) = \langle \chi | (I \otimes O) | \chi \rangle$ pour tout O . Cette matrice est appelée matrice de densité associée à $|\chi\rangle$. Elle est entièrement définie par sa propriété sur les observables.

Voyons quelques propriétés sur les matrices de densité.

Tout d'abord, si $|\chi\rangle = |\phi\rangle \otimes |\psi\rangle$ est un état séparable, alors $\rho = |\psi\rangle\langle\psi|$. Ceci nous permettra de reformuler rapidement les principes de la mécanique quantique en termes d'opérateurs de densité. Par ailleurs, on appelle état pur un état décrit par une matrice de densité pouvant se mettre sous la forme $|\psi\rangle\langle\psi|$.

Un opérateur de densité est positif et de trace 1. En effet, pour tout opérateur positif p , on a $Tr(p\rho) = \langle \chi | I \otimes p | \chi \rangle \geq 0$ puisque $I \otimes p$ est également positif. De plus, $Tr(\rho) = Tr(\rho I) = \langle \chi | I \otimes I | \chi \rangle = \langle \chi | \chi \rangle = 1$.

Enfin, l'opération de trace partielle $|\chi\rangle \mapsto \rho$ peut être définie sur les opérateurs de densité de $H_1 \otimes H_2$ par $\tilde{\rho} \in \mathcal{L}(H_1 \otimes H_2) \mapsto \rho \in \mathcal{L}(H_2)$, où ρ est l'unique opérateur tel que pour toute observable A , $Tr(A\rho) = Tr((I \otimes A)\tilde{\rho})$.

Définition 5.1 : Opérateurs purs

On appelle opérateur pur tout opérateur de densité se mettant sous la forme $|\psi\rangle\langle\psi|$. C'est donc une projection de rang 1.

On appelle opérateur mixte tout opérateur de densité qui n'est pas pur.

5.1.6 Reformulation des principes en termes d'opérateurs de densité

Probabilité de mesurer λ et état après mesure

Au niveau de la mesure, p_λ est maintenant donné par $Tr(P_\lambda\rho)$ (qui vaut $\langle \chi | I \otimes P_\lambda | \chi \rangle$). De plus, après mesure, on obtient un nouvel état $\rho' = \frac{P_\lambda\rho P_\lambda}{p_\lambda}$.

En effet, le nouvel état est $|\chi'\rangle = \frac{(I \otimes P_\lambda)|\chi\rangle}{\sqrt{p_\lambda}}$. (L'égalité des probabilités est donnée par définition.) Donc ρ' est l'unique opérateur tel que pour toute observable A ,

$$\begin{aligned} Tr(A\rho') &= \langle \chi' | I \otimes A | \chi' \rangle = \frac{1}{p_\lambda} \langle \chi | (I \otimes P_\lambda)(I \otimes A)(I \otimes P_\lambda) | \chi \rangle \\ &= \frac{1}{p_\lambda} \langle \chi | I \otimes (P_\lambda A P_\lambda) | \chi \rangle = \frac{1}{p_\lambda} Tr(P_\lambda A P_\lambda \rho) \\ &= \frac{1}{p_\lambda} Tr(AP_\lambda \rho P_\lambda) \end{aligned}$$

On a bien $\rho' = \frac{P_\lambda \rho P_\lambda}{p_\lambda}$.

États séparables

Il reste à définir ce que sont les états séparables en termes d'opérateurs de densité quand on couple deux systèmes. Soient S_1, S_2 les deux systèmes que l'on couple et S_e leur environnement. Un état séparable de $S = S_1 \cup S_2$ s'écrit $|\psi\rangle \otimes |\phi\rangle$. Un état de $S_e \cup S$, pour lequel la partie relative à S est séparable se note $\sum_i \alpha_i |\chi_i\rangle \otimes (|\psi_i\rangle \otimes |\phi_i\rangle)$. La trace partielle de ce vecteur est $\sum_i |\alpha_i|^2 |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$. Un état séparable est donc un opérateur appartenant à l'enveloppe convexe de l'ensemble $\{\rho_1 \otimes \rho_2\}$ où ρ_i est un opérateur de densité de H_i .

En effet, les $\sum_i |\alpha_i|^2 |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$ forment l'enveloppe convexe des $|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|$. Or, tout opérateur de densité ρ_1 se met sous la forme $\rho_1 = \sum_i t_i |\psi_i\rangle\langle\psi_i|$ avec $t_i \geq 0$, $\sum_i t_i = 1$ et donc l'opérateur

$$\rho_1 \otimes \rho_2 = \sum_{i,j} t_i t_j' |\psi_i\rangle\langle\psi_i| \otimes |\phi_j\rangle\langle\phi_j|$$

est dans l'enveloppe convexe des $|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|$.

5.1.7 Transformations admissibles, superopérateurs

Bien entendu, au même titre qu'en mécanique classique l'état d'un système (p, q) est une fonction du temps, les opérateurs de densité ρ évoluent. Plutôt que décrire leur évolution temporelle, donnée par l'équation de Schrödinger, on va s'intéresser à la forme générale des transformations admises par ces opérateurs.

Tout d'abord, en passant outre le phénomène de mesure, l'évolution des systèmes est linéaire, on va donc se limiter aux transformations linéaires F de $\mathcal{L}(H)$.

De plus, un opérateur de densité doit rester un opérateur de densité, ce qui nous donne deux conditions supplémentaires. Si ρ est positif, alors $F(\rho)$ l'est également. De plus, si $Tr(\rho) = 1$ alors $Tr(F(\rho)) = 1$.

N'oublions pas que ρ et $F(\rho)$ sont des traces partielles. Autrement dit, il existe x et x' positifs de trace 1 tel que pour tout A , $Tr(A\rho) = Tr(I \otimes Ax)$ et $Tr(AF(\rho)) = Tr(I \otimes Ax')$. Or,

$$Tr(AF(\rho)) = Tr(F^\dagger(A)\rho) = Tr((I \otimes F^\dagger(A))x) = Tr((Id \otimes F)^\dagger(I \otimes A)x)$$

$$Tr(I \otimes Ax') = Tr((I \otimes A)((Id \otimes F)(x)))$$

On impose de plus que pour tout espace H' , l'application $Id_{H'} \otimes F$ stabilise également l'ensemble des opérateurs de densité de $H' \otimes H$. De cette façon, quand on couple le système à un autre système, on conserve une évolution qui envoie les positifs vers les positifs.

On appelle ces applications des applications superpositives ou superopérateurs.

5.1.8 Principe de non-clonage

Insistons sur le fait qu'en mécanique quantique, on ne peut pas "copier" d'états.

En effet, si on dispose d'un état ρ , il n'existe aucune transformation quantique qui envoie ρ sur $\rho \otimes \rho$, tout simplement car cette application n'est pas linéaire, et ne peut pas dépendre d'une mesure puisqu'elle n'implique aucune perte d'information.

Autrement dit, lorsqu'on dispose d'une transformation sur les états, on ne peut pas "récupérer" l'état de départ avec le résultat, car cela signifierait de factoriser la transformation par une transformation du type $\rho \mapsto \rho \otimes \rho$.

5.2 Intrication

Il existe un lien entre l'intrication et les superopérateurs, que ce soit en logique ou en algèbre linéaire. En effet, l'existence d'états intriqués est équivalente à l'existence d'applications positives (qui stabilisent l'ensemble des matrices positives) qui ne sont pas des superopérateurs.

L'exemple type de ces applications est la **transposition**. C'est grâce à elle qu'on peut détecter si un état est intriqué. Cependant, elle ne suffit pas à caractériser l'intrication. On verra pourtant plus tard qu'elle permet de voir si une application positive est superpositive ou non.

Avant de poursuivre, rappelons que $\mathcal{L}(H_1) \otimes \mathcal{L}(H_2)$ est canoniquement isomorphe à $\mathcal{L}(H_1 \otimes H_2)$ par l'application linéaire qui, à $\rho_1 \otimes \rho_2$ associe l'opérateur :

$$|u\rangle \otimes |v\rangle \mapsto (\rho_1|u\rangle) \otimes (\rho_2|v\rangle).$$

De plus, rappelons quelques notations.

Définition 5.2 : O

n

appelle norme d'opérateur et on note $\|\cdot\|_2$ la norme sur les opérateurs associée au produit scalaire sur les opérateurs, c'est-à-dire que pour tout $U \in \mathcal{H}_\infty$, $\|U\|_2^2 = Tr(U^*U)$.

On appelle norme triple et on note $\|\|\|\cdot\|\|\|$ la norme sur les opérateurs associée au produit scalaire sur les vecteurs, c'est-à-dire que pour tout $U \in \mathcal{H}_\infty$,

$$\|\|\|U\|\|\|^2 = \max \left\{ \frac{\langle Ux|Ux\rangle}{\langle x|x\rangle} \mid |x\rangle \neq 0 \right\}.$$

5.2.1 Critère d'Horodecki

On se donne deux espaces de Hilbert H_1 et H_2 et on forme leur produit tensoriel $H = H_1 \otimes H_2$. On cherche à caractériser les états séparables de H . Pour cela, on dispose du critère d'Horodecki.

Théorème 1 : critère d'Horodecki

Soit ρ un opérateur de densité de H . L'état ρ est séparable si et seulement si pour toute application positive $\Lambda : \mathcal{L}(H_2) \rightarrow \mathcal{L}(H_1)$, l'opérateur $(Id_{\mathcal{L}(H_1)} \otimes \Lambda)(\rho) \in \mathcal{L}(H_1 \otimes H_1)$ est positif.

On ne fera pas la démonstration du critère d'Horodecki dans le cadre de ce mémoire mais son énoncé permet de voir le lien entre superopérateur et intrication.

Supposons qu'on ait un état intriqué ρ . Alors il existe une application positive Λ telle que $(Id \otimes \Lambda)(\rho)$ ne soit pas positif. Autrement dit, Λ n'est pas un superopérateur.

Maintenant, supposons qu'il existe Λ de $\mathcal{L}(H_2)$ dans $\mathcal{L}(H_1)$ positive mais non superpositive. Cela signifie qu'il existe H' tel que $Id_{H'} \otimes \Lambda$ ne soit pas positif. Autrement dit, il existe $\rho \in \mathcal{L}(H' \otimes H_2)$ et $p \in \mathcal{L}(H' \otimes H_1)$ deux opérateurs positifs tels que $Tr((Id \otimes \Lambda)(\rho)p) < 0$. p se met sous la forme :

$$p = \sum_{i,j} x_{i,j} \otimes |e_i\rangle\langle e_j|$$

où les $|e_i\rangle$ forment une base orthonormée de H_1 . On pose $f : \mathcal{L}(H_1) \rightarrow \mathcal{L}(H')$ telle que $f(|e_i\rangle\langle e_j|) = x_{i,j}$.

L'application $y \mapsto Tr(\rho(f \otimes Id_{\mathcal{L}(H_2)})y)$ est une forme linéaire, positive sur les positifs. En effet, l'opérateur p étant positif, l'application f est superpositive (cf. commentaires en 10, p est égale à l'opérateur χ_F défini dans cette section). En particulier, $f \otimes Id_{\mathcal{L}(H_2)}$ est positive. Donc pour tout y positif, $(f \otimes Id_{\mathcal{L}(H_2)})(y)$ est positif, et comme ρ l'est également, $Tr(\rho(f \otimes Id_{\mathcal{L}(H_2)})y) \geq 0$.

On en déduit qu'il existe $\rho' \in \mathcal{L}(H_1 \otimes H_2)$ positif tel que $Tr(\rho'y) = Tr(\rho(f \otimes Id_{H_2})y)$. En particulier pour $y = (Id_{H_1} \otimes \Lambda^\dagger) \left(\sum_{i,j} |e_i\rangle\langle e_j| \otimes |e_i\rangle\langle e_j| \right)$, cela donne :

$$Tr(\rho'y) = Tr((Id \otimes \Lambda)(\rho') \sum_{i,j} |e_i\rangle\langle e_j| \otimes |e_i\rangle\langle e_j|)$$

Or,

$$Tr(\rho'y) = Tr(\rho(f \otimes Id)y) = Tr(\rho(Id \otimes \Lambda^\dagger) \circ (f \otimes Id) \left(\sum_{i,j} |e_i\rangle\langle e_j| \otimes |e_i\rangle\langle e_j| \right))$$

$$Tr(\rho'y) = Tr(\rho(Id \otimes \Lambda^\dagger)p) = Tr((Id \otimes \Lambda)(\rho)p) < 0$$

Finalement,

$$Tr((Id \otimes \Lambda)(\rho') \sum_{i,j} |e_i\rangle\langle e_j| \otimes |e_i\rangle\langle e_j|) = Tr((Id \otimes \Lambda)(\rho)p) < 0$$

Comme l'opérateur $\sum_{i,j} |e_i\rangle\langle e_j| \otimes |e_i\rangle\langle e_j|$ est positif, l'opérateur $(Id \otimes \Lambda)(\rho')$ ne l'est pas, et donc ρ' n'est pas séparable.

Conclusion : on a un état ρ' de $H_1 \otimes H_2$ non séparable.

On verra plus tard qu'on peut utiliser une adjonction entre applications linéaires sur les opérateurs et opérateurs pour détecter si une application est superpositive ou non. Avec la remarque précédente, on peut imaginer détecter la séparabilité grâce à la notion de superpositivité, elle-même détectable grâce à une transposition particulière. Or, nous allons voir que se limiter à une transposition (et donc à une base) ne suffit pas.

5.2.2 Transposition et intrication

On utilise en général la transposition pour détecter si un état est séparable. En effet, cette application est positive sans être superpositive. Autrement dit, elle détecte certains états intriqués. Cependant, la transposée est relative à une base, ce qui lui donne un côté subjectif.

Soit deux espaces de Hilbert H_1 et H_2 ainsi qu'une base orthonormée de $H_1 : (|e_i\rangle)$. La transposition relative à cette base est l'application linéaire de $\mathcal{L}(H_1)$ telle que $T(|e_i\rangle\langle e_j|) = |e_j\rangle\langle e_i|$ pour tout couple (i, j) .

Montrons que cette application est positive.

Soit x un opérateur positif et $|v\rangle$ un vecteur de H_1 . On décompose x en $\sum x_{i,j}|e_i\rangle\langle e_j|$. On a :

$$\langle v|T(x)|v\rangle = \sum_{i,j} x_{i,j} \langle v|e_j\rangle\langle e_i|v\rangle$$

Posons $|\bar{v}\rangle = \sum_i \langle v|e_i\rangle \cdot |e_i\rangle$ qui est le conjugué de $|v\rangle$ dans la base e_i , on a $\langle \bar{v}|e_i\rangle = \langle e_i|v\rangle$.

$$\langle v|T(x)|v\rangle = \sum_{i,j} x_{i,j} \langle \bar{v}|e_i\rangle\langle e_j|\bar{v}\rangle = \langle \bar{v}|x|\bar{v}\rangle \geq 0$$

Donc $T(x)$ est positif, T est une application positive.

Montrons qu'en revanche T n'est pas une application superpositive.

Il faut pour cela que H_2 soit au moins de dimension 2. On choisit alors $|v_1\rangle$ et $|v_2\rangle$ deux vecteurs orthogonaux de norme 1 de H_2 et on pose :

$$x := (|v_1\rangle\langle v_1| \otimes |e_1\rangle\langle e_1| + |v_2\rangle\langle v_2| \otimes |e_2\rangle\langle e_2|) (|v_1\rangle\langle v_1| + |v_2\rangle\langle v_2|)$$

Cet opérateur est un projecteur orthogonal, donc positif. Il se réécrit :

$$x = |v_1\rangle\langle v_1| \otimes |e_1\rangle\langle e_1| + |v_2\rangle\langle v_2| \otimes |e_2\rangle\langle e_2| + |v_1\rangle\langle v_2| \otimes |e_1\rangle\langle e_2| + |v_2\rangle\langle v_1| \otimes |e_2\rangle\langle e_1|$$

On en déduit :

$$(Id \otimes T)(x) = |v_1\rangle\langle v_1| \otimes |e_1\rangle\langle e_1| + |v_2\rangle\langle v_2| \otimes |e_1\rangle\langle e_2| + |v_1\rangle\langle v_2| \otimes |e_2\rangle\langle e_1| + |v_2\rangle\langle v_1| \otimes |e_2\rangle\langle e_2|$$

Montrons que cet opérateur n'est pas positif. En effet, son action sur $|w\rangle = |v_2\rangle \otimes |e_1\rangle - |v_2\rangle \otimes |e_2\rangle$ donne :

$$(Id \otimes T)(x)|w\rangle = -|v_2\rangle \otimes |e_1\rangle + |v_2\rangle \otimes |e_1\rangle = -|w\rangle$$

donc

$$\langle w|(Id \otimes T)(x)|w\rangle = -\langle w|w\rangle < 0$$

Conclusion : T n'est pas superpositive.

Cependant, $(Id \otimes T)$ transforme certains opérateurs intriqués en opérateurs positifs. En effet, en posant $|f_1\rangle = \frac{1}{\sqrt{2}}(|e_1\rangle + i|e_2\rangle)$ et $|f_2\rangle = \frac{1}{\sqrt{2}}(|e_1\rangle - i|e_2\rangle)$, on a $\langle f_i|f_j\rangle = \delta_{i,j}$. Autrement dit, les $|f_j\rangle$ sont orthonormés, on peut donc compléter $|f_1\rangle, |f_2\rangle$ en une base orthonormée tout comme $(|e_i\rangle)$. On en déduit que le projecteur y sur $(|v_1\rangle \otimes |f_1\rangle + |v_2\rangle \otimes |f_2\rangle)$ est intriqué, car on peut refaire les mêmes calculs que pour x en prenant la transposition relative à la base $(|f_j\rangle)$

Par contre,

$$|f_1\rangle\langle f_2| = \frac{1}{2}(|e_1\rangle\langle e_1| + i|e_1\rangle\langle e_2| + i|e_2\rangle\langle e_1| + |e_2\rangle\langle e_2|)$$

et donc

$$T(|f_1\rangle\langle f_2|) = |f_1\rangle\langle f_2|$$

On en déduit que $(Id \otimes T)(y) = y$ et est donc positif. La transposition ne détecte pas l'état intriqué décrit par y .

Ceci est assez étonnant compte tenu du fait que l'on détecte la superpositivité grâce à la transposition.

5.3 Exemples

Cette partie donne quelques exemples qui seront utiles pour la suite.

5.3.1 Spin n , symétries

Un spin n est un moment intrinsèque qui peut prendre pour valeurs $-n, -(n-1), \dots, n$, où n est entier ou demi-entier. On se place donc dans un espace de Hilbert de dimension $2n+1$.

La matrice de spin, diagonale, s'écrit

$$S = \begin{pmatrix} -n & & & & \\ & \ddots & & & \\ & & n-1 & & \\ & & & \ddots & \\ & & & & n \end{pmatrix}$$

Les particules ayant un spin entier (les bosons) se comportent de façon symétrique. Par exemple, si l'on dispose de deux bosons évoluant dans H_1 et $H_2 = H_1$, l'état du système est invariant sous la transformation $\sigma : |v\rangle \otimes |w\rangle \mapsto |w\rangle \otimes |v\rangle$. Par exemple, pour un système à deux bosons, les états symétriques de base sont : $|-1, -1\rangle$; $\frac{1}{\sqrt{2}}(|-1, 0\rangle + |0, -1\rangle)$; $\frac{1}{\sqrt{2}}(|-1, 1\rangle + |1, -1\rangle)$; $|0, 0\rangle$; $\frac{1}{\sqrt{2}}(|1, 0\rangle + |0, 1\rangle)$; et $|1, 1\rangle$.

En revanche, les particules ayant un spin demi-entier (les fermions) se comportent de façon antisymétrique. L'état du système est invariant sous la transformation : $|v\rangle \otimes |w\rangle \mapsto -|w\rangle \otimes |v\rangle$. Par exemple, un système à deux électrons admet pour unique état $\frac{1}{\sqrt{2}}(|-, +\rangle - |+, -\rangle)$.

En particulier, deux fermions ne peuvent pas être dans le même état car la projection de $|v\rangle \otimes |v\rangle$ sur le sous espace vectoriel des états antisymétriques est nul. On parle de principe d'exclusion de Pauli.

5.3.2 Symétries et dimension

On va voir qu'il existe un isomorphisme entre l'espace à n spins $\frac{1}{2}$ symétrisés et un spin $\frac{n}{2}$.

Vis à vis des remarques faites plus haut, on peut se demander pourquoi on considère les spins symétrisés et non anti-symétrisés. Une particule (un système) n'est pas décrite entièrement par son spin. En particulier, chaque vecteur décrivant un système admet une partie spatiale, $|\phi\rangle$, évoluant dans un espace de Hilbert de dimension infinie. Cette partie spatiale contient l'information quant à la probabilité que le système se trouve dans une position ou une autre.

L'état du système est alors représenté par $|\phi\rangle \otimes |s\rangle$, où $|s\rangle$ est la partie relative au spin. C'est cet état global qui doit être antisymétrique et non juste $|s\rangle$. Or, si $|\phi\rangle$ est elle-même antisymétrique, pour que l'état global le soit également, il faut et il suffit que la partie relative au spin, $|s\rangle$, soit symétrique.

En général, on s'arrange pour confiner les systèmes étudiés dans un potentiel imposant à la partie spatiale d'être antisymétrique (ce qui revient à avoir des fonctions d'ondes impaires) de façon à ce que la partie relative au spin soit symétrique.

Espace symétrique

Introduisons tout d'abord l'espace à n spins symétrisés. Soit $H_{1/2} = \text{Vect}(|+\rangle, |-\rangle)$, et $H_t = H_{1/2}^{\otimes n}$ l'espace à n spins.

Pour toute permutation σ de $1, \dots, n$, on appelle P_σ l'application linéaire sur H_t telle que $P_\sigma(|v_1, \dots, v_n\rangle) = |v_{\sigma(1)}, \dots, v_{\sigma(n)}\rangle$, avec pour convention $|w_1, \dots, w_n\rangle = |w_1\rangle \otimes \dots \otimes |w_n\rangle$. Ces applications vérifient les propriétés suivantes :

- pour tout couple de permutation $\sigma, \sigma' : P_\sigma P_{\sigma'} = P_{\sigma\sigma'}$
- pour toute permutation : $P_\sigma^\dagger = P_\sigma^{-1} = P_{\sigma^{-1}}$

On pose alors $P := \frac{1}{n!} \sum_\sigma P_\sigma$. Il apparaît immédiatement que P est un projecteur orthogonal. On appelle H_s l'espace sur lequel il projette, H_s est un espace de Hilbert pour la restriction du produit scalaire. C'est l'espace à n spins symétrisés.

5.3.3 Observable de spin total

Les spins s'additionnent, si bien que l'observable associée au spin total du système à n spins est égale à :

$$S = \sum_i I_{H_{1/2}}^{\otimes(i-1)} \otimes S_{1/2} \otimes I_{H_{1/2}}^{\otimes(n-i)}$$

où $S_{1/2}$ est l'observable associée au spin $1/2$.

L'observable de spin total admet $n + 1$ valeurs propres : $-\frac{n}{2}, \dots, \frac{n}{2}$, avec pour espace propre associé à $\frac{n}{2} - k$, le sous-espace vectoriel E_k de H_t engendré par les vecteurs $|\varepsilon_1, \dots, \varepsilon_n\rangle$, avec $\varepsilon_i = \pm$ et tels que l'ensemble $\{i | \varepsilon_i = -\}$ soit de cardinal k .

Les vecteurs de E_k admettent tous la même projection sur H_s . L'observable S restreinte à H_s admet donc $n + 1$ vecteurs propres chacun associé à une valeur propre différente de la forme $\frac{n}{2} - k$.

Par ailleurs, l'observable $S_{n/2}$ associée au spin $n/2$ admet également $n + 1$ vecteurs propres associés aux valeurs propres $-\frac{n}{2}, \dots, \frac{n}{2}$.

L'isomorphisme entre $H_{n/2}$ et H_s est défini comme étant celui qui envoie le vecteur propre de $S_{n/2}$ associé à $\frac{n}{2} - k$ sur le vecteur propre de S associé à la même valeur propre.

Remarquons que le fait d'augmenter le nombre de particules dans un système revient à passer à la limite semi-classique. Il y a donc un lien entre le passage à la dimension infinie et le retour à des notions classiques.

5.3.4 Produit tensoriel de deux spins

On se donne deux spins n et m avec pour espace de Hilbert H_n et H_m et pour observables associées S_n et S_m . On suppose sans nuire à la généralité que $n \geq m$. Le système formé par les deux spins admet pour observable de spin total :

$$S := I_{2n+1} \otimes S_m + S_n \otimes I_{2m+1}$$

Cette observable admet $2(n + m) + 1$ valeurs propres, $-(n + m), \dots, n + m$ associés aux espaces propres $E_k = \text{Vect}(\{|i, j\rangle \mid |i| \leq n, |j| \leq m, i + j = k\})$. La valeur propre k a donc pour multiplicité le cardinal de l'ensemble $I_k := \{i \mid |i| \leq n, |k - i| \leq m\}$.

Montrons que ce cardinal est égal à celui de $L_k := \{l \mid n - m \leq l \leq n + m, |k| \leq l\}$.

Comme $|k| \leq n + m$, l'ensemble L_k est aussi $\{l \mid \max(n - m, |k|) \leq l \leq n + m\}$. Autrement dit,

$$\#L_k = \begin{cases} n + m - (n - m) + 1 = 2m + 1 & \text{si } |k| \leq n - m \\ n + m - |k| + 1 & \text{sinon} \end{cases}$$

Quand à I_k , il est égal à $\{i \mid -n \leq i \leq n, k - m \leq i \leq k + m\}$, car

$$|k - i| \leq m \Leftrightarrow -m \leq k - i \leq m \Leftrightarrow -m - k \leq -i \leq m - k \Leftrightarrow k - m \leq i \leq k + m.$$

$$I_k = \{i \mid \max(-n, k - m) \leq i \leq \min(k + m, n)\}$$

1^{er} cas : $k < m - n \leq 0$.

On a : $k - m < -n$ et $k + m \leq m \leq n$ donc $\#I_k = k + m - (-n) + 1 = n + m - |k| + 1$.

2^{ème} cas : $|k| \leq n - m$.

On a : $k - m \geq m - n - m = -n$ et $k + m \leq n - m + m = n$ donc $\#I_k = k + m - (k - m) + 1 = 2m + 1$.

3^{ème} cas : $k > n - m \geq 0$.

On a : $k - m > -m \geq -n$ et $k + m > n - m + m = n$ donc $\#I_k = n - (k - m) + 1 = n + m - |k| + 1$.

Finalement,

$$\#I_k = \begin{cases} 2m + 1 & \text{si } |k| \leq n - m \\ n + m - |k| + 1 & \text{sinon} \end{cases}$$

Conclusion : $\#L_k = \#I_k$.

Maintenant, considérons la somme directe $\bigoplus_{l=n-m}^{n+m} H_l$ de spins l pour $l = n - m, n - m + 1, \dots, n + m$

et l'observable sur cet espace $S' = \bigoplus_l S_l$, somme directe des observables de spin.

L'observable S' admet pour valeurs propres $k = -n - m, -n - m + 1, \dots, n + m$. L'espace propre associé à k est l'espace F_k engendré par les vecteurs $|l : k\rangle$, où l réfère au sous-espace H_l sur lequel on se place et k à la valeur propre du spin sur cet espace, et avec, bien entendu, $|k| \leq l$. La multiplicité de k est donc $\#L_k$.

Les espaces E_k et F_k ont donc la même dimension, ils sont isomorphes. Finalement, on obtient un

isomorphisme Φ entre $H_n \otimes H_m$ et $\bigoplus_{l=n-m}^{n+m} H_l$ respectant le spin, c'est-à-dire que si $|\psi\rangle$ a pour spin total

s dans $H_n \otimes H_m$, $\Phi(|\psi\rangle)$ a pour spin s dans $\bigoplus_{l=n-m}^{n+m} H_l$.

6 Du classique au quantique (en quittant la diagonale)

Espaces cohérents quantiques

Il s'agit maintenant d'étendre la construction à des objets quantiques. On a bien préparé le terrain en présentant tout sous forme de matrices et ce qu'il manque apparaît assez clairement : jusqu'à maintenant, toutes les matrices que l'on a considérées étaient diagonales, et donc commutaient toutes deux à deux.

La prochaine étape sera donc, après les "sous-ensembles probabilistes", d'étendre la construction à des "sous-ensembles non-commutatifs" en permettant aux matrices que l'on va considérer d'avoir des coefficients hors-diagonale. L'idée est la suivante : on va manipuler les sous-ensembles probabilistes de la section précédente, mais dont on a "oublié" dans quelle base ils se diagonalisent. Cependant, on veut toujours qu'il existe une version diagonalisée de notre ensemble, et que cette version diagonalisée corresponde à ce qu'on a vu dans la section 4, *i.e.*, que ses coefficients soient réels et compris entre 0 et 1.

La classe de matrices correspondant exactement à cette propriété est celle des *hermitiennes positives*, de norme inférieure ou égale à 1. On va partir de cette intuition pour poser les premières définitions concernant les **espaces cohérents quantiques**.

Définition 6.1 : Trame (quantique)

On appellera *trame* tout espace de Hilbert de dimension finie.

Définition 6.2 : Polarité

Si $|X|$ est une trame et $f, g \in \mathcal{H}(|X|)$ —l'ensemble des opérateurs hermitiens de $|X|$ —, on dira que f et g sont polaires si :

$$0 \leq \text{Tr}(fg) \leq 1, \text{ ce que l'on notera } f \perp\!\!\!\perp g$$

Ce qui permet de définir le *polaire* de $X \subseteq \mathcal{H}(|X|)$ comme dans le cas classique :

$$\sim X := \{y \in \mathcal{H}(|X|) \mid \forall x \in X, x \text{ et } y \text{ sont polaires}\}$$

On peut maintenant donner la définition d'un espace cohérent quantique, sans surprise :

Définition 6.3 : espace cohérent quantique

On appelle *espace cohérent quantique* (ECQ) de trame $|X|$ tout sous-ensemble X de $\mathcal{H}(|X|)$ égal à son bipolaire.

$$\textit{i.e.}, \text{ tel que } X = \sim\sim X$$

On peut s'arrêter un moment pour faire quelques remarques :

- L'aspect "quantique" de la construction apparaît clairement vu la section précédente : les opérateurs hermitiens positifs et de trace inférieure à 1 sont une généralisation des *opérateurs de densité*, qui servent à représenter l'état d'un système quantique.
- On peut avoir l'impression de ne pas être allés jusqu'au bout de l'analogie avec les espaces cohérents probabilistes, puisqu'on n'a pas imposé aux opérateurs d'être de norme au plus 1. Cette propriété émergera en fait naturellement comme duale de la propriété « trace au plus 1 ». On laisse donc la polarité faire le travail.
- De plus, on n'a pas imposé aux opérateurs d'être positifs. Comme annoncé dans l'introduction, ce point fait l'objet d'une discussion en section 10.

Pour finir, voyons quelques propriétés élémentaires de la polarité (qui ne sont pas vraiment spécifiques aux ECQ).

Lemme 6.4 :

1. La polarité est décroissante pour l'inclusion : $X \subseteq Y$ implique $\sim Y \subseteq \sim X$.
2. La bipolarité est donc croissante pour l'inclusion.
3. La polarité échange union et intersection : $\sim(X \cup Y) = \sim X \cap \sim Y$.
4. Pour tout X , $X \subseteq \sim\sim X$.
5. Pour tout X , $\sim X$ est un ECQ : $\sim\sim\sim X = \sim X$.

Preuve : Montrons 5., les autres dérivant directement de la définition.

“ \sim ” est décroissante pour l'inclusion. De plus, $X \subseteq \sim\sim X$ donc $\sim(\sim\sim X) \subseteq \sim X$. Comme $\sim X \subseteq \sim\sim(\sim X)$, on a bien $\sim\sim\sim X = \sim X$. ★

Corollaire 6.5 : ECQ engendré

| Pour tout $X \subseteq \mathcal{H}(|X|)$, $\sim\sim X$ est le plus petit ECQ contenant X .

Preuve : D'après le lemme $\sim\sim X = \sim(\sim X)$ est un ECQ. Si Z est un ECQ contenant X on a : $X \subseteq Z$ et donc par croissance de la polarité $\sim\sim X \subseteq \sim\sim Z = Z$. ★

7 Propriétés des ECQ

7.1 Polarité et géométrie : le théorème du Bipolaire

Jusqu'à maintenant, on n'a pas vraiment utilisé le nouveau cadre mathématique dans lequel on s'est placé : toutes les propriétés de la polarité et des espaces cohérents qu'on a vues pour le moment sont valables dans le cas classique.

Le théorème du Bipolaire va remédier à cela. Sa démonstration dépend de manière essentielle du théorème de Hahn-Banach (dans sa forme géométrique), qui est un théorème d'analyse des espaces de Banach (de Hilbert dans notre cas).

Théorème du Bipolaire :

$X \subseteq \mathcal{H}(|X|)$ est un ECQ si et seulement si :

1. X est non-vide.
2. X est convexe et fermé.
3. Si $\mathbb{N}.x \subseteq X$, alors $-x \in X$.
4. Si $x, y \in X$, $\lambda, \mu \geq 0$ et $\lambda x + \mu y \in X$ alors $\lambda x \in X$.

Preuve : (on notera $(x | y)$ pour $Tr(xy)$ tout au long de la preuve)

On commence par supposer que X est égal à son bipolaire.

1. Tout ensemble de la forme $\sim Y$ contient 0, donc $X = \sim\sim X$ est non vide.
2. Tout ensemble de la forme $\sim Y$ est une intersection de fermés (préimages de $[0, 1]$ par les $(. | x)$ pour $x \in Y$, continues) et est convexe par linéarité de $(. | .)$.
3. Si $\mathbb{N}.x \subseteq X$, pour tout $y \in \sim X$ on a : $(\mathbb{N}.x \perp y) \subseteq [0, 1]$, donc $(x | y) = (-x | y) = 0$ et $-x \in \sim\sim X = X$.
4. Soient $x, y \in \sim\sim X$ et $\lambda, \mu \geq 0$ tels que $\lambda x + \mu y \in X$. Si $z \in \sim X$ on a $(\lambda x + \mu y | z) \leq 1$, $(x | z) \geq 0$ et $(y | z) \geq 0$, ce qui impose $(\lambda x | z) \leq 1$. Donc $\lambda x \in \sim\sim X = X$.

Supposons maintenant les propriétés 1–4 vérifiées pour X .

Soit $I := \{x \in X \mid \mathbb{N}x \subseteq X\}$. I forme un sous-espace vectoriel de $\mathcal{H}(|X|)$, on peut donc considérer I^\perp (pour le produit scalaire défini par la trace).

On pose, de plus $X' := X \cap I^\perp$.

Commençons par montrer que X' est compact : raisonnons par l'absurde et supposons qu'il existe (x_n) une suite dans X' telle que $(x_n | x_n) \rightarrow \infty$. On pose $z_n := \frac{x_n}{\sqrt{(x_n | x_n)}}$ et, comme $(z_n | z_n) = 1$, quite à en extraire une sous-suite, la suite z_n converge vers $z \in \mathcal{H}(|X|)$.

Montrons que pour tout $m \in \mathbb{N}$, l'opérateur mz appartient à X .

Considérons pour cela la suite mz_n qui converge vers mz .

On a $mz_n = \frac{m}{\sqrt{(x_n | x_n)}} x_n$. Or, la suite $(x_n | x_n)$ diverge. Donc à partir d'un certain rang, $\frac{m}{\sqrt{(x_n | x_n)}}$ est compris entre 0 et 1. On en déduit par convexité de X , qu'à partir d'un certain rang, la suite mz_n est à valeurs dans X . Par fermeture de X , sa limite appartient à X .

On a donc pour tout $m \in \mathbb{N}$, $mz \in X$. Autrement dit, $z \in I$.

De plus, $z_n \in I^\perp$ et $(z_n | z_n) = 1$ pour tout n . Donc on a également $z \in I^\perp$ et $(z | z) = 1$. Ce qui est absurde puisque $I \cap I^\perp = \{0\}$.

X' est donc fermé (intersection de deux fermés) et borné, il est compact.

De plus, $X \subseteq X' + I$ car si on décompose $x \in X$ sur I, I^\perp on obtient : $x = x_I + x_{I^\perp}$. Par 3., $-x_I \in I \subseteq X$.

On en déduit que $\frac{1}{2}x_{I^\perp} = \frac{1}{2}x + \frac{1}{2}(-x_I)$ appartient à X par convexité. De plus, on a :

$$2(\frac{1}{2}x_{I^\perp}) + x_I = x \in X$$

D'après 4., on a $x_{I^\perp} = 2(\frac{1}{2}x_{I^\perp}) \in X$. Enfin, $x_{I^\perp} \in I^\perp$, donc x_{I^\perp} appartient à X' . On a bien $X \subseteq X' + I$.

On sait déjà que $X \subseteq \sim\sim X$, montrons maintenant que le complémentaire de X est inclus dans celui de $(\sim\sim X)$:

Soit $y \notin X$. Le théorème de Hahn-Banach fournit un z tel que $(z | y) < 0$ et $(z | X) \geq 0$. En particulier $(z | I) \geq 0$ et donc (I est un espace vectoriel) $(z | I) = \{0\}$.

Donc $(z | X) = (z | X')$ car on a montré que $X \subseteq X' + I$ et $(z | I) = 0$, $(z | X)$ est donc borné par un certain M car X' est compact. On pose alors $z' := \frac{z}{M}$. $(z' | X) \in [0, 1]$, donc $z' \in \sim X$.

Comme $(z' | y) < 0$, $z' \not\in y$ et donc $y \notin \sim\sim X$. ★

On passe ainsi d'une caractérisation interactive des ECQ —des sous-ensembles de $\mathcal{H}(|X|)$ qui se comportent bien vis-à-vis de leur polaire— à une caractérisation purement géométrique.

7.2 Applications linéaires et produit tensoriel

Dans ce qui suit, on va décrire l'isomorphisme qui permet d'identifier les applications linéaires de $\mathcal{L}(H_1)$ dans $\mathcal{L}(H_2)$ et les opérateurs de $H_1 \otimes H_2$. Cela permettra de voir l'ECQ $X \rightarrow Y$ à la fois comme « les applications linéaires de X dans Y » et comme $\sim X \wp Y$.

Lemme 7.1 : $\mathcal{L}(H_1, H_2) \simeq H_2 \otimes H_1^*$

Si H_1 et H_2 sont des espaces de Hilbert de dimension finie, on peut identifier “canoniquement” (sans faire référence à une base) l'espace des applications linéaires de H_1 dans H_2 et $H_2 \otimes H_1^*$

Preuve : l'application définie sur les tenseurs purs par $|x\rangle \otimes \langle y| \rightarrow |x\rangle\langle y|$ est un isomorphisme quand la dimension est finie : il suffit de le vérifier sur une base de H_1 et sa base duale. ★

Théorème 2 : $\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)^6 \simeq \mathcal{L}(H_1 \otimes H_2)$

Si H_1 et H_2 sont des espaces de Hilbert de dimensions finies, l'espace des applications linéaires de $\mathcal{L}(H_1)$ dans $\mathcal{L}(H_2)$ est isomorphe à celui des opérateurs de $H_1 \otimes H_2$
Si $F \in \mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$, on notera θ_F l'opérateur de $H_1 \otimes H_2$ correspondant.
Inversement, si $x \in \mathcal{L}(H_1 \otimes H_2)$, on notera $[x]$ son image par l'isomorphisme.

Preuve : le lemme 7.1 permet de reformuler le théorème : on a

$$\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2) \simeq \mathcal{L}(H_1 \otimes H_1^*, H_2 \otimes H_2^*) \simeq H_2 \otimes H_2^* \otimes (H_1 \otimes H_1^*)^* \simeq H_2 \otimes H_2^* \otimes H_1^* \otimes H_1$$

et

$$\mathcal{L}(H_1 \otimes H_2) \simeq H_1 \otimes H_2 \otimes (H_1 \otimes H_2)^* \simeq H_1 \otimes H_2 \otimes H_1^* \otimes H_2^*$$

On est donc ramené à la commutativité (à isomorphisme près) du produit tensoriel. ★

La propriété suivante nous sera très utile, car elle relie la trace et l'isomorphisme. On aurait d'ailleurs pu directement définir l'isomorphisme à partir d'elle.

⁶Pour alléger les notations, on notera souvent $E \rightarrow F$ l'espace des applications linéaires de E vers F . Plus généralement, si $A \subseteq E$ et $B \subseteq F$ sont des sous-ensembles quelconques de E et F , $A \rightarrow B$ désignera l'ensemble des applications linéaires ϕ de E vers F telles que $\phi(A) \subseteq B$.

Proposition 7.2 :

|| Sous les hypothèses du théorème précédent on a, pour tout $\phi \in \mathcal{L}(H_1 \otimes H_2)$:

$$\text{Pour tous } x \in \mathcal{L}(H_1) \text{ et } y \in \mathcal{L}(H_2), \text{ Tr}(\phi(x \otimes y)) = \text{Tr}([\phi](x)y)$$

Preuve : du point de vue de l'identification du lemme 7.1, la trace est l'application linéaire de $H_1 \otimes H_1^*$ dans \mathbb{C} dont la valeur sur les tenseurs purs est donnée par $|x\rangle \otimes \langle y| \rightarrow \langle x|y\rangle$.

Prenons maintenant $\phi = |u \otimes v\rangle \langle u' \otimes v'|$, $x = |w\rangle \langle w'|$ et $y = |z\rangle \langle z'|$.

$$\text{Tr}(\phi(x \otimes y)) = \text{Tr}(|u \otimes v\rangle \langle u' \otimes v'| |w\rangle \langle w'| |z\rangle \langle z'|) = \langle u'|w\rangle \langle v'|z\rangle \cdot \langle w'|u\rangle \langle z'|v\rangle$$

Comme $[\phi] = |v\rangle \otimes \langle v'| \otimes \langle u'| \otimes |u\rangle$, $[\phi](x) = |v\rangle \otimes \langle v'| \cdot \langle u'|w\rangle \cdot \langle w'|u\rangle$, on obtient

$$\text{Tr}([\phi](x)y) = \langle z'|v\rangle \cdot \langle v'|z\rangle \cdot \langle u'|w\rangle \cdot \langle w'|u\rangle = \text{Tr}(\phi(x \otimes y))$$

Comme la relation est linéaire en u, u', v, v', z, \dots et comme les endomorphismes de rang 1 engendrent tous les endomorphismes, on a le résultat. ★

Enfin, on vérifie que l'isomorphisme est bien compatible avec les opérateurs hermitiens, dans le sens suivant :

Corollaire 7.3 : $\mathcal{H}(H_1) \rightarrow \mathcal{H}(H_2) \simeq \mathcal{H}(H_1 \otimes H_2)$

|| Toujours sous les mêmes hypothèses, $F \in \mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$ préserve les hermitiens si et seulement si θ_F est hermitien.

On en déduit que l'on a un isomorphisme entre $\mathcal{H}(H_1) \rightarrow \mathcal{H}(H_2)$ et $\mathcal{H}(H_1 \otimes H_2)$.

Preuve : D'après 7.2,

$$\text{Tr}([\phi](x)^\dagger y) = \text{Tr}([\phi](x)y^\dagger) = \text{Tr}(\phi(x \otimes y^\dagger)) = \text{Tr}(\phi^\dagger(x^\dagger \otimes y)) = \text{Tr}([\phi^\dagger](x^\dagger)y)$$

Donc, ceci valant pour tout y , $([\phi](x))^\dagger = [\phi^\dagger](x^\dagger)$. (■)

On en déduit que si θ_F est hermitien, pour tout $x \in \mathcal{H}(H_1)$, $([\phi](x))^\dagger = [\phi^\dagger](x^\dagger) = [\phi](x)$. C'est à dire $[\phi](x)$ hermitien.

Donc $[\cdot]$ envoie (injectivement) $\mathcal{H}(H_1 \otimes H_2)$ dans $\mathcal{H}(H_1) \rightarrow \mathcal{H}(H_2)$.

Réciproquement, si $F(\mathcal{H}(H_1)) \subseteq \mathcal{H}(H_2)$, alors F vérifie pour tout x (pas forcément hermitien, on passe pour cela par la décomposition de $\mathcal{L}(H_1)$ en "hermitiens \oplus anti-hermitiens") :

$$F(x^\dagger)^\dagger = F(x)$$

Mais alors, comme $F = [\theta_F]$, on utilise (■) :

$$\text{pour tout } x \in \mathcal{L}(H_1), [\theta_F^\dagger](x) = ([\theta_F](x^\dagger))^\dagger = F(x^\dagger)^\dagger = [\theta_F](x).$$

$$\text{Donc } \theta_F^\dagger = \theta_F.$$

Pour la dernière partie du théorème, on remarque que toute application linéaire F de $\mathcal{H}(H_1)$ dans $\mathcal{H}(H_2)$ peut être étendue de manière unique⁷ en un élément \mathbf{F} de $\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$ qui préserve les hermitiens en posant : $\mathbf{F}(g) := \frac{1}{2}(F(g + g^\dagger) + i.F(ig - ig^\dagger))$ puis en appliquant la première partie du résultat à \mathbf{F} . ★

Exemple : calculons à quoi correspond l'identité de $\mathcal{H}(H_1) \rightarrow \mathcal{H}(H_1)$.

Soit σ , le "flip" de $H_1 \otimes H_1$ défini sur les tenseurs purs par $\sigma(x \otimes y) = y \otimes x$.

On a : $\text{Tr}([\sigma](f)g) = \text{Tr}(\sigma(f \otimes g))$.

Dans le cas d'opérateurs de rang 1 :

$$\text{Tr}(\sigma(|u\rangle \langle v| \otimes |w\rangle \langle z|)) = \text{Tr}(|w\rangle \langle v| \otimes |u\rangle \langle z|) = \text{Tr}(|w\rangle \langle v|) \cdot \text{Tr}(|u\rangle \langle z|)$$

⁷On identifiera à partir de maintenant les deux notions.

Ceci vaut 0 sauf si $|w\rangle = |v\rangle$ et $|u\rangle = |z\rangle$. Or, $\text{Tr}(|u\rangle\langle v||w\rangle\langle z|)$ vaut également 0 sauf si $|w\rangle = |v\rangle$ et $|u\rangle = |z\rangle$.

On en déduit par linéarité que $\text{Tr}([\sigma](f)g) = \text{Tr}(fg)$, et donc que $[\sigma] = \text{Id}_{\mathcal{H}(H_1)}$

7.3 Connecteurs

On dispose maintenant de tous les outils nécessaires pour décrire les connecteurs des ECQ.

7.3.1 Additifs

Définition 7.4 :

Si A et B sont deux ECQ de trames respectives $|A|$ et $|B|$, on définit les ECQ⁸ $A \oplus B$ et $A \& B$ de la façon suivante :

$$A \oplus B := \{\lambda x \oplus \mu y \mid \lambda, \mu \geq 0, \lambda + \mu \leq 1, x \in A \text{ et } y \in B\}$$

$$A \& B := \{h \mid p_{|A|} h p_{|A|} \in A \text{ et } p_{|B|} h p_{|B|} \in B\}$$

(où p_E désigne la projection orthogonale sur le sous-espace E)

Proposition 7.5 : $\&$ est le polaire de \oplus

|| Si A et B sont deux ECQ, on a :

$$A \& B = \sim(\sim A \oplus \sim B)$$

Preuve : soit $h \in \mathcal{H}(|A| \oplus |B|)$, on pose $h_A := p_{|A|} h p_{|A|}$ et $h_B := p_{|B|} h p_{|B|}$.

- Si $h \in A \& B$, $h_A \in A$ et $h_B \in B$. Par conséquent, si $g = \lambda x \oplus \mu y \in A \oplus B$ on calcule $\text{Tr}(gh) = \lambda \text{Tr}(x h_A) + \mu \text{Tr}(y h_B) \in [0, 1]$, et donc $h \in \sim(\sim A \oplus \sim B)$.
- Si $h \notin A \& B$, on a $h_A \notin A$ ou $h_B \notin B$. Supposons que ce soit h_A (le problème étant symétrique) : il existe alors un $x \in A$ tel que $h_A \not\leq x$. On a alors $x \oplus 0_{|B|} \in \sim A \oplus \sim B$ et $h \not\leq x \oplus 0_{|B|}$, donc $h \notin \sim(\sim A \oplus \sim B)$.

★

On peut voir l'espace $A \oplus B$ comme un mélange statistique des états de A et de ceux de B : l'état décrit par $(ta \oplus (1-t)b)$ est a avec probabilité t et b avec probabilité $(1-t)$; mais comme la réunion de deux Hamiltoniens dont on ne peut pas passer continûment des états propres de l'un aux états propres de l'autre.

Plus précisément : supposons que l'on dispose de deux puits de potentiel à supports disjoints caractérisés par les potentiels V_a et V_b . On suppose donc que V_a et V_b sont infinis en dehors de deux régions de l'espace Ω_a et Ω_b telles que $\Omega_a \cap \Omega_b = \emptyset$. Le potentiel H_2 total est donné par :

$$V(x) = \begin{cases} V_a(x) & \text{si } x \in \Omega_a \\ V_b(x) & \text{si } x \in \Omega_b \\ \infty & \text{sinon} \end{cases}$$

Le système physique que l'on étudie est par exemple au départ confiné dans Ω_a . À une date donnée, on impose $V = 0$ et on laisse le système évoluer librement. Il se délocalise alors dans tout l'espace. (en particulier dans Ω_b) Puis on impose à nouveau le potentiel composé des deux puits (ce qui consiste d'une certaine manière à faire une **mesure sans lecture**) de façon à confiner le système dans $\Omega = \Omega_a \cup \Omega_b$. On obtient ainsi des matrices de densité diagonales par bloc sur les espaces d'évolution de V_a et V_b .

⁸Ce sont bien des ECQ, par le théorème du **bipolaire**.

7.3.2 Multiplicatifs

Définition 7.6 :

Si A et B sont deux ECQ de trames respectives $|A|$ et $|B|$, on pose :

$$A \otimes B := \sim\sim\{x \otimes y \mid x \in A \text{ et } y \in B\}$$

On définit le \wp par dualité :

$$A \wp B := \sim(\sim A \otimes \sim B).$$

On en déduit également une définition de l'ECQ associé à l'implication linéaire :

$$A \multimap B := \sim A \wp B$$

Si les choses ont été bien faites on devrait retrouver un lien avec un point de vue “applications linéaires de A dans B ” pour l'implication linéaire au travers de l'isomorphisme décrit précédemment. C'est bien le cas :

Théorème 3 :

Soient A et B deux espaces cohérents, on a :

$$A \multimap B = \{\theta_F \mid F \in A \rightarrow B\}$$

(θ_F est défini en 7.2)

Preuve :

Soit $F \in A \rightarrow B$. Le polaire de $A \multimap B = \sim A \wp B$ étant $A \otimes \sim B = \sim\sim\{x \otimes y \mid x \in A \text{ et } y \in \sim B\}$, il suffit de montrer que $\theta_F \perp x \otimes y$ pour tous $x \in A$ et $y \in \sim B$ pour avoir $\theta_F \in A \multimap B$.

Or, par la proposition 7.2, pour $x \in \mathcal{H}(|A|)$ et $y \in \mathcal{H}(|B|)$, $Tr(\theta_F(x \otimes y)) = Tr(F(x)(y))$.

Mais alors si $x \in A$ et $y \in \sim B$, comme $F \in A \rightarrow B$, $F(x) \in B$ et $F(x) \perp y$.

Donc $Tr(\theta_F(x \otimes y)) \in [0, 1]$. Ceci valant pour tous x et y , on a bien $\theta_F \in \sim(A \otimes \sim B) = A \multimap B$.

Réciproquement, soit F tel que $\theta_F \in A \multimap B$. Soit $x \in A$. Pour montrer que $F(x) \in B$ on va montrer que $F(x) \perp y$ pour tout y dans $\sim B$.

Soit donc $y \in \sim B$, toujours par la proposition 7.2, $Tr(F(x)y) = Tr(\theta_F(x \otimes y)) \in [0, 1]$ car $\theta_F \in A \multimap B = \sim(A \otimes \sim B)$. ★

Alors que le \otimes se présente comme l'enveloppe convexe des opérateurs s'écrivant comme un produit tensoriel $\rho_1 \otimes \rho_2$, le \wp va autoriser plus de mélange entre les deux espaces. On verra cela plus clairement dans l'exemple de la section 8.

7.3.3 Distributivité

Les connecteurs satisfont un isomorphisme attendu en logique linéaire :

Proposition 7.7 : distributivité

\otimes distribue sur \oplus , :

$$\text{pour tous } A, B, C \quad A \otimes (B \oplus C) \simeq (A \otimes B) \oplus (A \otimes C)$$

Dualement, \wp distribue sur $\&$.

On commence par montrer le lemme suivant :

Lemme 7.8 :

Soit φ un isomorphisme unitaire entre deux trames $|A|$ et $|B|$. On déduit de ϕ un isomorphisme entre les opérateurs hermitiens de $|A|$ et ceux de $|B|$:

$$\phi : \rho \mapsto \varphi \rho \varphi^{-1}$$

Cet isomorphisme vérifie les propriétés suivantes :

1. ϕ préserve la trace : pour tout $f \in \mathcal{L}(|A|)$, $Tr(\phi(f)) = Tr(f)$.
2. ϕ préserve donc la polarité : si X est un ensemble d'hermitiens sur $|A|$, $\phi(\sim X) = \sim \phi(X)$.
3. En particulier, on a la propriété suivante : si X est un ensemble d'hermitiens sur $|A|$ et Y un ensemble d'hermitiens sur $|B|$, tels que $\phi(X) \subseteq Y$, on a $\phi(\sim \sim X) \subseteq \sim \sim Y$.

Preuve : ϕ est bien un isomorphisme entre $\mathcal{H}(|A|)$ et $\mathcal{H}(|B|)$, car φ étant unitaire, $\varphi^\dagger = \varphi^{-1}$ et donc si h est hermitien, $\varphi h \varphi^{-1} = \varphi h \varphi^\dagger$ l'est également.

Notation : on écrira $|\phi(x)\rangle$ pour $\phi(|x\rangle)$ et également $\langle \phi(x)|$ pour la forme linéaire associée.

Soit $h \in \mathcal{H}(|A|)$ et $(|b_1\rangle, \dots, |b_n\rangle)$ une base orthonormée de $|B|$.

On a $Tr(\phi(h)) = \sum_{i=1}^n \langle \varphi^{-1}(b_i) | h | \varphi^{-1}(b_i) \rangle$. Mais φ^{-1} étant unitaire, $(|\varphi^{-1}(b_1)\rangle, \dots, |\varphi^{-1}(b_n)\rangle)$ est une base orthonormée de $|A|$ et donc la somme est aussi égale à $Tr(h)$.

Comme $Tr(\phi(f)\phi(g)) = Tr(\varphi f \varphi^{-1} \varphi g \varphi^{-1}) = Tr(\varphi f g \varphi^{-1}) = Tr(fg)$, on a $f \sim g$ si et seulement si $\phi(f) \sim \phi(g)$. On en déduit que $\phi(\sim X) = \sim \phi(X)$.

Enfin, **3.** s'obtient en utilisant **2.** : $\phi(\sim \sim X) = \sim \sim \phi(X)$ puis par croissance de la bipolarité par rapport à l'inclusion $\phi(\sim \sim X) = \sim \sim \phi(X) \subseteq \sim \sim Y$. ★

Preuve de la distributivité : on applique le lemme avec φ l'isomorphisme habituel entre $|A| \otimes (|B| \oplus |C|)$ et $|A| \otimes |B| \oplus |A| \otimes |C|$.

Posons $X_1 := \{a \otimes (b \oplus 0_{|C|}) \mid a \in A, b \in B\}$ et $X_2 := \{a \otimes (0_{|B|} \oplus c) \mid a \in A, c \in C\}$.

On a $\phi(X_1) \subseteq \{a \otimes b \oplus 0_{|A \otimes |C|}\} \subseteq A \otimes B \oplus A \otimes C$.

De même, $\phi(X_2) \subseteq A \otimes B \oplus A \otimes C$.

Donc par le point **3.** du lemme et le fait que $\sim \sim (X_1 \cup X_2) = |A| \otimes (|B| \oplus |C|)$, on a $\phi(|A| \otimes (|B| \oplus |C|)) \subseteq |A| \otimes |B| \oplus |A| \otimes |C|$

Le même type de raisonnement donne l'inclusion inverse. ★

7.3.4 Éléments neutres

On trouve également des ECQ qui sont des éléments neutres (à isomorphisme près) des connecteurs que l'on vient de lister.

Définition 7.9 : $1, \perp$

1 et \perp sont deux ECQ de trame \mathbb{C} tous les deux égaux au segment $[0, 1]$.

Définition 7.10 : $0, \top$

0 et \top sont deux ECQ de trame $\{0\}$, forcément égaux à $\{0\}$.

Il est immédiat que $\sim 1 = \perp$ et $\sim 0 = \top$.

De plus $1, \perp, 0$ et \top sont des éléments neutres. Plus précisément :

Proposition 7.11 : éléments neutres

On a les isomorphismes suivants, pour tout ECQ X :

1. $X \otimes 1 \simeq X$
2. $X \wp \perp \simeq X$
3. $X \& \top \simeq X$
4. $X \oplus 0 \simeq X$

Preuve : évident, l'isomorphisme sur les trames étant à peu de choses près l'identité.



8 Un exemple-clé : les booléens quantiques

Le premier exemple d'ECQ donné par Jean-Yves Girard sont les booléens quantiques. Il s'agit d'une extension de l'ensemble des matrices de densité. En effet, l'ensemble des matrices de densité, comme il ne contient que des matrices de trace 1, ne contient pas l'opérateur nul. Afin de remédier à ce problème, Jean-Yves Girard définit le booléen quantique comme étant l'ensemble des matrices positives de trace comprise entre 0 et 1.

Remarquons que P. Selinger choisit également un système dans lequel la représentation des états autorise une trace inférieure à 1. En effet, il raisonne en terme de transformation. Une transformation correspond dans son système à un algorithme. Or, un algorithme ne termine pas toujours. Cette liberté sur la trace permet d'envisager une non terminaison⁹.

Définition 8.1 :

Soit H un espace de Hilbert. On pose :

- $P_H := \{ \rho \geq 0 \mid 0 \leq \text{Tr}(\rho) \leq 1 \}$
- $N_H := \{ n \geq 0 \mid \|n\| \leq 1 \}$

Qu'on appellera respectivement booléens et anti-booléens quantiques.

Ces deux espaces sont polaires l'un de l'autre :

Proposition 8.2 :

|| On a : $P_H = \sim N_H$ et $N_H = \sim P_H$, ce qui fait de P_H et N_H des espaces cohérents quantiques.

Preuve : Tout d'abord montrons que $P_H = \sim N_H$.

Inclusion $P_H \subset \sim N_H$.

Soit $\rho \in P_H$ et $n \in N_H$. Comme ρ est positif, on a $\text{Tr}(\rho n) \geq 0$. Par ailleurs,

$$\text{Tr}(\rho n) \leq \|n\| \text{Tr}(\rho) \leq \text{Tr}(\rho) \leq 1.$$

Donc ρ est dans le polaire de N_H .

Réciproquement, si ρ est dans le polaire de N_H , comme pour tout vecteur $|v\rangle$ de norme 1, le projecteur $|v\rangle\langle v|$, est dans N_H , on a :

$$\langle v|\rho|v\rangle = \text{Tr}(\rho|v\rangle\langle v|) \in [0, 1].$$

Donc ρ est positif. De plus, l'identité appartient à N_H donc $\text{Tr}(\rho) = \text{Tr}(\rho Id) \in [0, 1]$. Le polaire de N_H est bien inclus dans P_H .

Passons à la deuxième égalité.

On a déjà montré l'inclusion $N_H \subseteq \sim P_H$, en montrant la première inclusion dans l'égalité précédente. Il reste à voir que le polaire de P_H est inclus dans N_H .

Soit n dans le polaire de P_H . Pour tout vecteur $|v\rangle$ de norme 1, le projecteur $|v\rangle\langle v|$ est dans P_H donc $\langle v|n|v\rangle = \text{Tr}(n|v\rangle\langle v|) \in [0, 1]$, on en déduit que n est positif. Diagonalisons n . On pose $n = \sum_i \lambda_i |\phi_i\rangle\langle \phi_i|$. Les projecteurs $|\phi_i\rangle\langle \phi_i|$ appartiennent à P_H , donc pour tout i , on a $\lambda_i = \text{Tr}(n|\phi_i\rangle\langle \phi_i|) \in [0, 1]$, toutes les valeurs propres de n sont prises entre 0 et 1, on a bien $0 \leq n \leq Id$. ★

8.1 Par et intrication

Avant de décrire le \mathfrak{F} des booléens quantiques, intéressons nous au tenseur. En effet, il se trouve que le tenseur de deux booléens correspond à une extension des états séparables sur l'espace produit tensoriel des deux trames. Plus précisément :

⁹Voir l'annexe A.2 pour plus de détails.

Proposition 8.3 :

Soient H_1 et H_2 deux espaces de Hilbert. On note Sep l'ensemble des matrices de densité représentant un état séparable de $H_1 \otimes H_2$, ie Sep est l'enveloppe convexe de l'ensemble $A := \{\rho_1 \otimes \rho_2 \mid \forall i \rho_i \geq 0, Tr(\rho_i) = 1\}$. On a alors :

$$P_{H_1} \otimes P_{H_2} = [0, 1]Sep \quad (1)$$

Preuve : Commençons par montrer que $[0, 1]Sep$ est un espace cohérent quantique. Pour cela, on utilise le théorème du Bipolaire.

1. $0 \in [0, 1]Sep$.
2. Sep est convexe et fermé par définition et $[0, 1]$ aussi donc $[0, 1]Sep$ est un convexe fermé.
3. $[0, 1]Sep$ est borné donc vérifie automatiquement la condition $\forall x, Nx \subseteq [0, 1]Sep \Rightarrow -x \in [0, 1]Sep$.
4. Soient $x, y \in [0, 1]Sep$ et $\lambda, \mu \geq 0$ tels que $\lambda x + \mu y \in [0, 1]Sep$, montrons que $\lambda x \in [0, 1]Sep$. Soient $x', y' \in Sep$ et $a, b \in [0, 1]$ tels que $x = ax'$ et $y = by'$. On a

$$Tr(\lambda x + \mu y) = \lambda a + \mu b \in [0, 1]$$

et $\lambda a, \mu b \geq 0$ donc $\lambda a \in [0, 1]$. On en déduit, $\lambda x = \lambda ax' \in [0, 1]Sep$.

Montrons que $[0, 1]Sep \subseteq P_{H_1} \otimes P_{H_2}$.

En effet, $P_{H_1} \otimes P_{H_2}$ contient A et est convexe, donc il contient son enveloppe convexe Sep . De plus, il contient 0, et donc également l'enveloppe convexe de $\{0\} \cup Sep$, c'est-à-dire, $[0, 1]Sep$.

Montrons que $\sim[0, 1]Sep \subseteq \sim(P_{H_1} \otimes P_{H_2})$.

On a :

$$\sim(P_{H_1} \otimes P_{H_2}) = \sim\{\rho_1 \otimes \rho_2 \mid \rho_i \in P_{H_i}\}$$

En effet, pour tout ensemble X , on a montré que $\sim\sim X = \sim X$ et donc, $(P_{H_1} \otimes P_{H_2})$ étant le bipolaire de $\{\rho_1 \otimes \rho_2 \mid \rho_i \in P_{H_i}\}$, on a :

$$\sim(P_{H_1} \otimes P_{H_2}) = \sim\sim\sim\{\rho_1 \otimes \rho_2 \mid \rho_i \in P_{H_i}\}$$

$$\sim(P_{H_1} \otimes P_{H_2}) = \sim\{\rho_1 \otimes \rho_2 \mid \rho_i \in P_{H_i}\}.$$

Or, pour tout $\rho_i \in P_{H_i}$, on peut écrire $\rho_i = a_i \rho'_i$ avec $a_i \in [0, 1]$ et $Tr(\rho'_i) = 1$. En effet, si $Tr(\rho_i) = 0$ alors comme ρ_i est positif, il est nul, et donc on peut écrire $\rho_i = 0|\nu\rangle\langle\nu|$ où $|\nu\rangle$ est un vecteur quelconque de norme 1. Sinon, on pose $a_i := Tr(\rho_i)$ et $\rho'_i = \frac{\rho_i}{a_i}$.

Pour tout $\rho_i \in P_{H_i}$, on a alors,

$$\rho_1 \otimes \rho_2 = a_1 a_2 \rho'_1 \otimes \rho'_2$$

avec $a_1 a_2 \in [0, 1]$ et $\rho'_1 \otimes \rho'_2 \in Sep$. On en déduit que $\{\rho_1 \otimes \rho_2 \mid \rho_i \in P_{H_i}\} \subseteq [0, 1]Sep$, et donc que son polaire

$$\sim\{\rho_1 \otimes \rho_2 \mid \rho_i \in P_{H_i}\} = \sim(P_{H_1} \otimes P_{H_2})$$

contient le polaire de $[0, 1]Sep$.

Conclusion : $[0, 1]Sep = \sim\sim[0, 1]Sep = \sim\sim(P_{H_1} \otimes P_{H_2}) = P_{H_1} \otimes P_{H_2}$. ★

Le tenseur ne permettant pas aux états d'être intriqués, on s'imagine que le \mathfrak{N} va permettre de réaliser l'intrication. En effet, on a interprété le \mathfrak{N} comme un mélange indisociable de deux composants, comme deux produits en solution. Or, l'intrication en mécanique quantique est une notion d'indisociabilité. Elle témoigne d'un partage d'information entre deux systèmes, si bien qu'agir sur l'un modifie l'état de l'autre, et ce même s'ils n'interagissent plus à travers un Hamiltonien les couplant (par exemple, s'ils sont à trop grande distance l'un de l'autre pour se "voir" à travers une interaction). On verra qu'on retrouve des états intriqués dans le \mathfrak{N} , mais aussi des opérateurs qui ne sont pas positifs.

Par exemple, si $H_1 = H_2$, L'identité de $\mathcal{L}(H_1)$ divisée par la dimension n_1 de H_1 envoie les opérateurs de norme (triple) inférieure à 1 sur les opérateurs de trace inférieure à 1, donc l'opérateur $\phi \in \mathcal{L}(H_1 \otimes H_2)$ défini par $\phi := \theta_{Id/n_1}$ est dans $N_{H_1} \rightarrow P_{H_1} \mathfrak{N} P_{H_1}$.

Or, ϕ n'est pas positif. En effet, soient $|v\rangle, |w\rangle$ deux vecteurs orthogonaux de norme 1 de H_1 , on a :

$$\begin{aligned} (\langle v, w| - \langle w, v|)\phi(|v, w\rangle - |w, v\rangle) &= Tr(\phi|v, w\rangle\langle v, w|) \\ &\quad + Tr(\phi|w, v\rangle\langle w, v|) \\ &\quad - Tr(\phi|v, w\rangle\langle w, v|) \\ &\quad - Tr(\phi|w, v\rangle\langle v, w|) \end{aligned}$$

Or,

$$Tr(\phi|v, w\rangle\langle v, w|) = Tr(\phi|v\rangle\langle v| \otimes |w\rangle\langle w|) = Tr(|v\rangle\langle v||w\rangle\langle w|)/n_1 = 0$$

et

$$Tr(\phi|v, w\rangle\langle w, v|) = Tr(\phi|v\rangle\langle w| \otimes |w\rangle\langle v|) = Tr(|v\rangle\langle w||w\rangle\langle v|)/n_1 = 1/n_1$$

donc

$$(\langle v, w| - \langle w, v|)\phi(|v, w\rangle - |w, v\rangle) = -2/n_1 < 0$$

Conclusion : ϕ appartient à $P_{H_1} \mathfrak{N} P_{H_2}$ et n'est pas positif. Le \mathfrak{N} réalise en fait plus que l'intrication de deux systèmes.

Le \mathfrak{N} admet deux définitions équivalentes. D'une part, on peut le voir comme le polaire du tenseur, c'est-à-dire $A \mathfrak{N} B = \sim((\sim A) \otimes (\sim B))$, ou comme une implication linéaire, c'est-à-dire $A \mathfrak{N} B = (\sim A) \rightarrow B$.

On s'intéresse ici au \mathfrak{N} de deux booléens quantiques. On se donne donc deux espaces de Hilbert H_1 et H_2 et on note P_{H_1} et P_{H_2} leurs espaces de booléens respectifs. Posons $P = P_{H_1} \mathfrak{N} P_{H_2}$.

La première définition du \mathfrak{N} permet de voir P comme le polaire de $N_{H_1} \otimes N_{H_2}$, ou encore le polaire de l'ensemble $\{n_1 \otimes n_2 | n_1 \in N_{H_1}, n_2 \in N_{H_2}\}$.

On voit alors immédiatement les conditions nécessaires suivantes pour appartenir à P :

Lemme 8.4 :

Soit $\rho \in P$. Pour tout $|v\rangle \in H_1$ et $|w\rangle \in H_2$, on a :

$$\langle v| \otimes \langle w|\rho|v\rangle \otimes |w\rangle \geq 0 \tag{2}$$

De plus, $Tr(\rho) \leq 1$.

Preuve : Soit $|v\rangle, |w\rangle$ deux vecteurs de norme 1 appartenant respectivement à H_1 et H_2 . On a $|v\rangle\langle v| \in N_{H_1}$ et $|w\rangle\langle w| \in N_{H_2}$, donc

$$\langle v| \otimes \langle w|\rho|v\rangle \otimes |w\rangle = Tr(\rho|v\rangle\langle v| \otimes |w\rangle\langle w|) \geq 0$$

De plus Id_{H_i} est dans N_{H_i} pour tout i donc

$$Tr(\rho) = Tr(\rho Id_{H_1 \otimes H_2}) = Tr(\rho Id_{H_1} \otimes Id_{H_2}) \leq 1$$

★

Ces conditions donnent en fait une caractérisation des éléments de P . En effet,

Théorème 4 :

- Soit ρ un opérateur hermitien de $H_1 \otimes H_2$. On a $\rho \in P$ si et seulement si :
- $Tr(\rho) \leq 1$
 - pour tout $|v\rangle \in H_1$ et $|w\rangle \in H_2$, $\langle v| \otimes \langle w| \rho |v\rangle \otimes |w\rangle \geq 0$.

Preuve : Il reste à montrer l'implication réciproque. On suppose que ρ vérifie (2) et $Tr(\rho) \leq 1$. Montrons que ρ appartient à P .

Soit $n_1 \in N_{H_1}$ et $n_2 \in N_{H_2}$ et diagonalisons les dans des bases orthonormées. On note :

$$n_1 = \sum_i \lambda_i |v_i\rangle\langle v_i|,$$

$$n_2 = \sum_j \mu_j |w_j\rangle\langle w_j|.$$

Calculons $Tr(\rho n_1 \otimes n_2)$.

$$\begin{aligned} Tr(\rho n_1 \otimes n_2) &= Tr(\rho (\sum_i \lambda_i |v_i\rangle\langle v_i|) \otimes (\sum_j \mu_j |w_j\rangle\langle w_j|)) \\ &= Tr(\rho (\sum_{i,j} \lambda_i \mu_j |v_i\rangle\langle v_i| \otimes |w_j\rangle\langle w_j|)) \\ &= \sum_{i,j} \lambda_i \mu_j Tr(\rho |v_i\rangle\langle v_i| \otimes |w_j\rangle\langle w_j|) \end{aligned}$$

D'une part,

$$Tr(\rho n_1 \otimes n_2) = \sum_{i,j} \lambda_i \mu_j \langle v_i| \otimes \langle w_j| \rho |v_i\rangle \otimes |w_j\rangle$$

or, $\lambda_i \geq 0$, $\mu_j \geq 0$ et $\langle v_i| \otimes \langle w_j| \rho |v_i\rangle \otimes |w_j\rangle \geq 0$. Donc

$$Tr(\rho n_1 \otimes n_2) \geq 0.$$

D'autre part, $\lambda_i, \mu_j \leq 1$ et $\langle v_i| \otimes \langle w_j| \rho |v_i\rangle \otimes |w_j\rangle \geq 0$ donc

$$\begin{aligned} Tr(\rho n_1 \otimes n_2) &\leq \sum_{i,j} Tr(\rho |v_i\rangle\langle v_i| \otimes |w_j\rangle\langle w_j|) \\ &\leq Tr(\rho \sum_{i,j} |v_i\rangle\langle v_i| \otimes |w_j\rangle\langle w_j|) \end{aligned}$$

Or, les $|v_i\rangle \otimes |w_j\rangle$ forment une base orthonormée de $H_1 \otimes H_2$, donc $\sum_{i,j} |v_i\rangle\langle v_i| \otimes |w_j\rangle\langle w_j| = Id$ et

$$Tr(\rho n_1 \otimes n_2) \leq Tr(\rho) \leq 1.$$

Conclusion : l'opérateur ρ appartient donc au polaire de l'ensemble $\{n_1 \otimes n_2 | n_1 \in N_{H_1}, n_2 \in N_{H_2}\}$ qui est égal à P . ★

Passons à la seconde description du \mathfrak{N} . On a $P = N_{H_1} \rightarrow P_{H_2}$. Autrement dit, le \mathfrak{N} correspond aux transformations linéaires vérifiant $F(x^\dagger) = (F(x))^\dagger$ qui envoient N_{H_1} dans P_{H_2} .

Lemme 8.5 :

Soit $\rho \in \mathcal{L}(H_1 \otimes H_2)$ hermitien et $F : \mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$ tel que $[F] = \rho$. On se donne une base orthonormée $|e_i\rangle$ de H_1 et on note $T : \mathcal{L}(H_1) \rightarrow \mathcal{L}(H_1)$ la transposition associée à cette base, c'est-à-dire la transformation linéaire telle que $T(|e_i\rangle\langle e_j|) = |e_j\rangle\langle e_i|$.

Il existe une base orthonormée $(U_i)_i$ de $\mathcal{L}(H_1, H_2)$ pour le produit scalaire $(x, y) = \text{Tr}(x^\dagger y)$, et des réels λ_i tels que :

$$F : x \mapsto \sum \lambda_i U_i T(x) U_i^\dagger \quad (3)$$

Preuve : L'opérateur ρ est hermitien, donc il se diagonalise dans une base orthonormée $(|\psi_i\rangle)_i$ de $H_1 \otimes H_2$. On pose alors λ_i la valeur propre associée à $|\psi_i\rangle$ et on décompose $|\psi_i\rangle$ en :

$$|\psi_i\rangle = \sum_j |e_j\rangle \otimes |v_j^i\rangle.$$

Posons : $U_i := \sum_j |v_j^i\rangle\langle e_j| \in \mathcal{L}(H_1, H_2)$.

Montrons que les U_i forment une base orthonormée de $\mathcal{L}(H_1, H_2)$. En effet,

$$\text{Tr}(U_i^\dagger U_j) = \sum_{k,l} \text{Tr}(|v_k^i\rangle\langle e_k| |e_l\rangle\langle v_l^j|) = \sum_k \langle v_k^i | v_k^j \rangle = \langle \psi_i | \psi_j \rangle = \delta_{i,j}$$

Montrons que $F : x \mapsto \sum_i \lambda_i U_i T(x) U_i^\dagger$. On a :

$$\sum_i \lambda_i U_i T(|e_k\rangle\langle e_l|) U_i^\dagger = \sum_i \lambda_i |v_l^i\rangle\langle v_k^i|$$

et

$$\begin{aligned} \rho &= \sum_i \lambda_i |\psi_i\rangle\langle \psi_i| \\ &= \sum_i \sum_k \sum_l \lambda_i |e_k\rangle\langle e_l| \otimes |v_k^i\rangle\langle v_l^i| \\ &= \sum_k \sum_l |e_k\rangle\langle e_l| \otimes \left(\sum_i \lambda_i |v_k^i\rangle\langle v_l^i| \right) \end{aligned}$$

On en déduit : $F(|e_k\rangle\langle e_l|) = \sum_i \lambda_i |v_k^i\rangle\langle v_l^i|$

On a bien la bonne forme de F . ★

De plus, on peut s'affranchir de la base.

Théorème 5 :

Soit $\rho \in \mathcal{L}(H_1 \otimes H_2)$ hermitien et F telle que $[\rho] = F$. Il existe une base orthonormée (U_i) de $\mathcal{L}(H_1, H_2)$ et des λ_i tels que $F : x \mapsto \sum_i \lambda_i U_i x U_i^\dagger$.

Preuve : On note G la transformation telle que $[(T \otimes Id)(\rho)] = G$. Cette transformation se met sous la forme

$$G : x \mapsto \sum_i \lambda_i U_i T(x) U_i^\dagger$$

Soit $x \in \mathcal{L}(H_1)$ et $y \in \mathcal{L}(H_2)$. Le calcul de $\text{Tr}(F(x)y)$ donne :

$$\begin{aligned} \text{Tr}(F(x)y) &= \text{Tr}(\rho x \otimes y) \\ &= \text{Tr}((T \otimes Id)(\rho) T(x) \otimes y) \end{aligned}$$

En effet, si on décompose ρ sous la forme $\rho = \sum_i \rho_i^1 \otimes \rho_i^2$, on a

$$\begin{aligned} (T \otimes Id)(\rho) &= \sum_i T(\rho_i^1) \otimes \rho_i^2 \\ (T \otimes Id)(\rho)(x \otimes y) &= \sum_i (T(\rho_i^1)x) \otimes (\rho_i^2 y) \\ Tr((T \otimes Id)(\rho)(x \otimes y)) &= \sum_i Tr(T(\rho_i^1)x) Tr(\rho_i^2 y) \\ &= \sum_i Tr(\rho_i^1 T(x)) Tr(\rho_i^2 y) = Tr((\sum_i \rho_i^1 \otimes \rho_i^2)(T(x) \otimes y)) = Tr(\rho T(x) \otimes y) \end{aligned}$$

Donc,

$$Tr(F(x)y) = Tr(G(T(x))y)$$

$$\text{donc pour tout } x, F(x) = G(T(x)) = \sum_i \lambda_i U_i x U_i^\dagger. \quad \star$$

Remarque : la preuve du théorème permet de voir que $(T \otimes Id)\rho$ est positif si et seulement si F est une application superpositive, c'est-à-dire une application telle que $(Id_H \otimes F)$ envoie les positifs dans les positifs pour tout espace H .

Remarque : l'application F est indépendante de la base choisie pour H_1 puisqu'elle est l'application vérifiant pour tout x, y , $Tr(F(x)y) = Tr(\rho x \otimes y)$, donc le choix des U_i est indépendant de la base de H_1 choisie.

Cherchons à présent des conditions sur les U_i telles que l'opérateur ρ soit dans P .

Théorème 6 :

Soit $\rho \in \mathcal{L}(H_1 \otimes H_2)$ hermitien et $F : x \mapsto \sum_i \lambda_i U_i x U_i^\dagger$ l'application linéaire de $\mathcal{L}(H_1)$ dans $\mathcal{L}(H_2)$. L'opérateur ρ appartient à P si et seulement si pour tout $|v\rangle \in H_1$ et $|w\rangle \in H_2$, on a :

$$\begin{cases} \sum_i \lambda_i |\langle w | U_i v \rangle|^2 \geq 0 \\ \sum_i \lambda_i \leq 1 \end{cases} \quad (4)$$

Preuve : on a vu que ρ était dans P si et seulement si $Tr(\rho) \leq 1$ et pour tout $|v\rangle \in H_1$ et $|w\rangle \in H_2$, on a :

$$\langle v | \otimes \langle w | \rho | v \rangle \otimes | w \rangle \geq 0.$$

La première condition se traduit par

$$\begin{aligned} 1 &\geq Tr(\rho) = Tr(\rho(Id \otimes Id)) = Tr(F(Id)Id) = Tr(\sum_i \lambda_i U_i U_i^\dagger) \\ &= \sum_i \lambda_i Tr(U_i^\dagger U_i) = \sum_i \lambda_i \end{aligned}$$

Et la deuxième par :

$$\begin{aligned} 0 &\leq \langle v | \otimes \langle w | \rho | v \rangle \otimes | w \rangle = Tr(\rho | v \rangle \langle v | \otimes | w \rangle \langle w |) \\ &= Tr(F(|v\rangle\langle v|) | w \rangle \langle w |) = \sum_i \lambda_i Tr(U_i | v \rangle \langle v | U_i^\dagger | w \rangle \langle w |) \\ &= \sum_i \lambda_i \langle w | U_i | v \rangle \langle v | U_i^\dagger | w \rangle = \sum_i \lambda_i |\langle w | U_i | v \rangle|^2 \end{aligned}$$

★

8.2 Valeurs propres négatives dans les ECQ

Par rapport à l'exemple type qu'on a donné précédemment, à savoir l'identité de $\mathcal{L}(H)$ divisée par la dimension, on pourrait s'attendre à ce que la borne inférieure valeurs propres négatives des opérateurs de $P_{H_1} \bowtie P_{H_2}$ tendent vers 0 quand la dimension de H_1 ou H_2 tend vers $+\infty$.

Nous allons voir qu'il n'en est rien.

Proposition 8.6 :

Soit H_1 et H_2 deux espaces de Hilbert et P_{H_1}, P_{H_2} leurs booléens respectifs. On suppose que la dimension de ces deux espaces de Hilbert est supérieure ou égale à 2. Alors il existe au moins un opérateur dans $P_{H_1} \bowtie P_{H_2}$ admettant pour valeur propre $-\frac{1}{2}$.

Preuve : Soit $|e_1\rangle$ et $|e_2\rangle$ deux vecteurs orthonormés de H_1 et $|f_1\rangle, |f_2\rangle$ deux vecteurs orthonormés de H_2 .

On complète $|e_i\rangle$ en une base orthonormée de H_1 et $|f_j\rangle$ en une base orthonormée de H_2 . On note alors P l'opérateur :

$$P = |e_1\rangle\langle f_1| + |e_2\rangle\langle f_2|$$

et on considère la transformation :

$$F : \rho \mapsto \frac{1}{2}P^*\rho P.$$

Cette application envoie les opérateurs positifs de norme triple inférieure ou égale à 1 de $\mathcal{L}(H_1)$ sur des opérateurs positifs de trace comprise entre 0 et 1 de $\mathcal{L}(H_2)$.

En effet, pour tout $\rho \geq 0$ de norme triple inférieure ou égale à 1 et $|x\rangle$ de H_2 , on a :

$$\langle x|F(\rho)|x\rangle = \frac{1}{2}\langle Px|\rho|Px\rangle \geq 0$$

et

$$\text{Tr}(F(\rho)) = \sum_j \langle f_j|F(\rho)|f_j\rangle = \frac{1}{2} \sum_{i=1,2} \langle e_i|\rho|e_i\rangle \leq 1.$$

L'opérateur θ tel que $[\theta] = F$ appartient donc à l'espace cohérent quantique $N_{H_1} \rightarrow P_{H_2} = P_{H_1} \bowtie P_{H_2}$.

Constatons à présent que θ admet pour valeur propre $-\frac{1}{2}$.

L'opérateur θ s'écrit :

$$\begin{aligned} \theta &= \frac{1}{2} \sum_{i,j=1,2} |e_i\rangle\langle e_j| \otimes |f_j\rangle\langle e_i| \\ \theta &= \frac{1}{2} \sum_{i,j=1,2} |e_i, f_j\rangle\langle e_j, f_i|. \end{aligned}$$

Soit $|v\rangle$ le vecteur $|v\rangle = |e_1, f_2\rangle - |e_2, f_1\rangle$. On a :

$$\theta|v\rangle = \frac{1}{2}|e_2, f_1\rangle - |e_1, f_2\rangle = -\frac{1}{2}|v\rangle.$$

Donc $\theta \in P_{H_1} \bowtie P_{H_2}$ admet $-\frac{1}{2}$ comme valeur propre.

★

Conclusion : les valeurs propres négatives des opérateurs de $P_{H_1} \bowtie P_{H_2}$ ne tendent pas vers 0 quand

la dimension tend vers $+\infty$.

8.3 Retour sur les cas classiques et probabilistes

Les Booléens classiques

On se donne une trame $|X|$, de cardinal n et on cherche construire un espace cohérent classique maximal tel que son interprétation en termes de matrice s'injecte dans un booléen quantique.

Définition 8.7 : booléens classiques

On définit le booléen classique relatif à $|X|$ noté $B_{|X|}$, l'ensemble

$$B_{|X|} = \{\emptyset\} \cup \{\{e\} \mid e \in |X|\}.$$

C'est un espace cohérent classique.

Son polaire est simplement l'ensemble des parties de $|X|$.

En effet, pour tout $x \subseteq |X|$, on a :

- $\#|x \cap \emptyset| = 0$,
- $\#|x \cap \{e\}| = 1$ si $e \in x$, 0 sinon.

Cet espace s'interprète en termes de matrices comme l'ensemble des matrices positives diagonales dont les coefficients sont 0 ou 1 de trace prise entre 0 et 1.

Supposons qu'il existe un espace cohérent X dans lequel $B_{|X|}$ est inclus strictement. Alors X contient au moins une paire $\{e_1, e_2\}$. Or, cette paire s'interprète comme une matrice de trace 2 n'appartenant donc pas au booléen quantique correspondant.

Par de deux espaces cohérents classiques

Soit X, Y deux espaces cohérents classiques de trames respectives $|X|$ et $|Y|$. On définit le \wp par polarité, c'est-à-dire comme le polaire de $\sim X \otimes \sim Y$.

Or l'ensemble $A \otimes B$ pour les espaces cohérents classiques est le bipolaire de l'ensemble :

$$\{a \times b \mid a \in A, b \in B\}.$$

On en déduit que $X \wp Y$ est donné par :

$$X \wp Y = \sim \{x \times y \mid x \in \sim X, y \in \sim Y\}.$$

Par de deux booléens classiques

On va montrer l'égalité suivante :

Proposition 8.8 :

Soit $|X|$ et $|Y|$ deux ensembles finis et $B_{|X|}, B_{|Y|}$ leurs booléens respectifs, on a :

$$B_{|X|} \wp B_{|Y|} = B_{|X| \times |Y|}.$$

Preuve : par définition, $B_{|X|} \wp B_{|Y|}$ est le polaire de $\{x \times y \mid x \in \sim B_{|X|}, y \in \sim B_{|Y|}\}$. Autrement dit, $\rho \subseteq |X| \times |Y|$ appartient à $B_{|X|} \wp B_{|Y|}$ si et seulement si pour tout $x \subseteq |X|$ et $y \subseteq |Y|$, on a :

$$\#|\rho| \cap (x \times y) \leq 1.$$

En particulier, si $\rho \in B_{|X|} \wp B_{|Y|}$, alors $\#|\rho| = \#|\rho| \cap |X| \times |Y| \leq 1$, donc $\rho \in \mathcal{B}_{|X| \times |Y|}$.

Réciproquement, si ρ appartient à $\mathcal{B}_{|X| \times |Y|}$. Alors, on a $\#|\rho| \leq 1$ et donc pour tout $x \subseteq |X|$ et $y \subseteq |Y|$, le cardinal de $\rho \cap x \times y$ est inférieur ou égal à celui de ρ et est donc inférieur à 1.

Conclusion : $B_{|X|} \wp B_{|Y|} = B_{|X| \times |Y|}$. ★

Cas probabiliste

Booléens probabilistes

Rappelons que les objets des espaces cohérents probabilistes sont des fonctions d'un ensemble fini $|X|$ dans $[0, 1]$. Et que, si f est une telle fonction et qu'on a numéroté les éléments de $|X|$: e_1, \dots, e_n , f s'interprète comme la matrice diagonale :

$$M_f = \begin{pmatrix} f(e_1) & & \\ & \ddots & \\ & & f(e_n) \end{pmatrix}$$

Définition 8.9 : Booléen probabiliste

Soit $|X|$ un ensemble fini. On appelle booléen probabiliste et on note $B_{|X|}^P$ l'ensemble :

$$B_{|X|}^P = \{f \mid \sum_{e \in |X|} f(e) \leq 1\}.$$

C'est un espace cohérent probabiliste.

Son polaire est l'ensemble $\{g \mid \forall e \in |X| g(e) \leq 1\}$.

En effet, si pour tout $e \in |X|$, $g(e) \leq 1$, alors pour tout $f \in B_{|X|}^P$,

$$Tr(M_f M_g) = \sum_{e \in |X|} f(e)g(e) \leq \sum_{e \in |X|} f(e) \leq 1$$

Réciproquement, pour tout $e \in |X|$, la fonction

$$f_e : e' \mapsto \begin{cases} 1 & \text{si } e=e' \\ 0 & \text{sinon} \end{cases}$$

représentée par la matrice diagonale :

$$M_{f_e} = \begin{pmatrix} \delta_{e,e_1} & & \\ & \ddots & \\ & & \delta_{e,e_n} \end{pmatrix}$$

appartient à $B_{|X|}^P$ donc si g appartient au polaire de $B_{|X|}^P$, on a

$$g(e) = Tr(M_{f_e} M_g) = \sum_{e' \in |X|} g(e')f_e(e') \leq 1.$$

L'espace $B_{|X|}^P$ s'interprète en termes de matrices comme l'ensemble des matrices diagonales positives de trace inférieure ou égale à 1.

De plus, si X est un espace cohérent probabiliste contenant strictement $B_{|X|}^P$, alors X contient au moins une fonction f telle que $\sum_{e \in |X|} f(e) > 1$. Or, l'interprétation matricielle de cette fonction admet une trace strictement supérieure à 1 et donc l'interprétation matricielle de X ne s'injecte pas dans les booléens quantiques.

Conclusion : $B_{|X|}^P$ est le plus grand espace cohérent probabiliste s'injectant dans le booléen quantique de trame associée à $|X|$.

Définition du par de deux espaces cohérents probabilistes

Une fois de plus, on regarde la définition par polarité.

Soit A et B deux espaces cohérents probabilistes de trames respectives $|A|$ et $|B|$. L'espace $A \otimes B$ est défini comme le bipolaire de l'ensemble :

$$\{a \otimes b \mid a \in A, b \in B\}$$

où $a \otimes b$ est la fonction qui à tout couple $e, e' \in |A| \times |B|$ associe le réel positif $a(e)b(e')$.

L'espace $X \wp Y = \sim(\sim X \otimes \sim Y)$ est donc le polaire de l'ensemble :

$$\{x \otimes y \mid x \in \sim X, y \in \sim Y\}.$$

Par de deux espaces cohérents probabilistes

On va montrer l'égalité analogue du cas classique.

Proposition 8.10 :

Soit $|X|$ et $|Y|$ deux ensembles finis et $B_{|X|}^P, B_{|Y|}^P$ leurs booléens respectifs. On a l'égalité suivante :

$$B_{|X|}^P \wp B_{|Y|}^P = \mathcal{B}_{|X| \times |Y|}^P.$$

Preuve : par définition, l'espace $B_{|X|}^P \wp B_{|Y|}^P$ est le polaire de l'ensemble des $x \otimes y$ tels que pour tout $e \in |X|$ et $e' \in |Y|$, $x(e) \leq 1$, $y(e') \leq 1$.

Soit $\rho \in B_{|X|}^P \wp B_{|Y|}^P$. Notons X la fonction qui à tout $e \in |X|$ associe 1 et Y celle qui à tout $e' \in |Y|$ associe 1. L'élément ρ est polaire à $X \otimes Y$ donc

$$\sum_{(e,e') \in |X| \times |Y|} \rho(e, e') = \sum_{(e,e') \in |X| \times |Y|} \rho(e, e') X \otimes Y(e, e') \leq 1$$

donc $\rho \in \mathcal{B}_{|X| \times |Y|}^P$.

Réciproquement, si $\rho \in \mathcal{B}_{|X| \times |Y|}^P$, alors

$$\sum_{(e,e') \in |X| \times |Y|} \rho(e, e') \leq 1$$

et donc pour tout x et y tels que $x(e) \leq 1$, $y(e') \leq 1$, on a

$$\sum_{(e,e') \in |X| \times |Y|} \rho(e, e') x(e) y(e') \leq \sum_{(e,e') \in |X| \times |Y|} \rho(e, e') \leq 1.$$

On en déduit $\rho \in B_{|X|}^P \wp B_{|Y|}^P$.

Conclusion : on a bien l'égalité $B_{|X|}^P \wp B_{|Y|}^P = \mathcal{B}_{|X| \times |Y|}^P$. ★

9 Un exemple qui se généralise

9.1 Espaces de Hilbert-Schmidt

Les espaces de Hilbert-Schmidt sont des espaces auto polaires, c'est-à-dire qu'ils vérifient $\sim X = X$. Ils sont définis grâce à la norme associée au produit scalaire.

Définition 9.1 :

Soit H un espace de Hilbert, on appelle espace de Hilbert-Schmidt l'ECQ :

$$HS_H = \{h \geq 0 \mid Tr(h^2) \in [0, 1]\}$$

Proposition 9.2 : $\sim HS_H = HS_H$

|| HS_H est égal à son polaire, ce qui prouve au passage qu'il s'agit bien d'un ECQ.

Preuve : montrons $\sim HS_H \subseteq HS_H$.

Soit $h \in \sim HS_H$ non nul. Pour tout opérateur positif g , $Tr(gh) \geq 0$ donc $h \geq 0$. Comme h est non nul, $Tr(h^2) = Tr(h^*h)$ est strictement positive, on peut donc poser $h' = \frac{h}{\sqrt{Tr(h^2)}}$. On a

$$Trh'^2 = \frac{Trh^2}{Trh^2} = 1 \text{ donc } h' \in HS_H.$$

On en déduit que $\sqrt{Tr(h^2)} = Tr(hh')$ appartient à $[0, 1]$. donc h est dans HS_H .

Réciproquement, si h est dans HS_H , alors par Cauchy Schwartz, pour tout g dans HS_H , on a :

$$Tr(gh) \leq \sqrt{Tr(h^2)Tr(g^2)} \leq 1$$

De plus, g et h sont positifs donc $Tr(gh) \geq 0$. On a bien $h \in \sim HS_H$. ★

Par de deux Hilbert-Schmidt

Soient H_1 et H_2 deux espaces de Hilbert. On pose HS_{H_1} et HS_{H_2} leur Hilbert-Schmidt respectifs et on s'intéresse à $HS_{H_1} \wp HS_{H_2}$.

En particulier, on va montrer qu'il contient des applications dont la norme triple relative aux normes associées au produit scalaire est inférieure à 1, ce qui n'est pas évident de prime abord compte tenu du fait que l'on a une condition uniquement sur les opérateurs positifs.

Posons $H := HS_{H_1} \wp HS_{H_2}$.

On sait que $H = HS_{H_1} \rightarrow HS_{H_2} = \{\theta = \theta^* \mid [\theta](HS_{H_1}) \subseteq HS_{H_2}\}$.

Lemme 9.3 :

| Soit $\theta \in H$ et $F = [\theta]$. Alors pour tout $x \in \mathcal{L}(H_1)$, on a $Tr(F(x)^*F(x)) \leq Tr(x^*x)$.

Preuve : 1^{er} cas : $x = 0$. On a $F(x) = 0$.

2^{ème} cas : $x > 0$. On pose $x' = \frac{x}{\sqrt{Tr(x^2)}}$. On a $Tr(x'^2) = 1$ donc $x' \in HS_{H_1}$, donc $F(x') \in HS_{H_2}$,

c'est-à-dire $\frac{Tr(F(x)^2)}{Tr(x^2)} = Tr\left(\frac{F(x)^2}{Tr(x^2)}\right) = Tr(F(x')^2) \in [0, 1]$, on a bien $Tr(F(x)^2) \leq Tr(x^2)$.

3^{ème} cas : x hermitien. L'opérateur x se diagonalise, il se met donc sous la forme $x = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$. On pose alors $|x| = \sum |\lambda_i| |\psi_i\rangle\langle\psi_i|$. On a $Tr(x^2) = Tr(|x|^2)$. De plus,

$$Tr(F(x)^2) = \sum \lambda_i \lambda_j Tr(F(|\psi_i\rangle\langle\psi_i|)F(|\psi_j\rangle\langle\psi_j|))$$

Or, F envoie les positifs sur les positifs donc pour tout couple i, j ,

$$Tr(F(|\psi_i\rangle\langle\psi_i|)F(|\psi_j\rangle\langle\psi_j|)) \geq 0$$

On en déduit

$$\text{Tr}(F(x)^2) \leq \sum |\lambda_i| |\lambda_j| \text{Tr}(F(|\psi_i\rangle\langle\psi_i|)F(|\psi_j\rangle\langle\psi_j|)) = \text{Tr}(F(|x|^2))$$

Finalement,

$$\text{Tr}(F(x)^2) \leq \text{Tr}(|x|^2) = \text{Tr}(x^2)$$

4^{ème} cas : x antihermitien. On a

$$\text{Tr}(F(x)^*F(x)) = \text{Tr}(-iF(x)^*iF(x)) = \text{Tr}((iF(x))^*(iF(x))) = \text{Tr}(F(ix)^*F(ix))$$

Or, ix est hermitien donc

$$\text{Tr}(F(x)^*F(x)) \leq \text{Tr}((ix)^*(ix)) = \text{Tr}(-ix^*ix) = \text{Tr}(x^*x)$$

Denier cas : x quelconque.

x se décompose en une partie hermitienne et une partie anti-hermitienne :

$$x = \frac{x + x^*}{2} + \frac{x - x^*}{2}$$

Posons $y = \frac{x+x^*}{2}$ et $z = \frac{x-x^*}{2}$. On a :

$$4F(y)^*F(y) = F(x)^2 + F(x^*)^2 + F(x)F(x^*) + F(x^*)F(x)$$

$$4\text{Tr}(F(y)^*F(y)) = \text{Tr}(F(x)^2) + \text{Tr}(F(x^*)^2) + 2\text{Tr}(F(x)^*F(x))$$

puisque $F(x^*) = F(x)^*$.

$$4F(z)^*F(z) = F(z^*)F(z) = -F(z)^2 = -(F(x)^2 + F(x^*)^2 - F(x)F(x)^* - F(x)^*F(x))$$

$$4\text{Tr}(F(z)^*F(z)) = -\text{Tr}(F(x)^2) - \text{Tr}(F(x^*)^2) + 2\text{Tr}(F(x)^*F(x))$$

d'où

$$\text{Tr}(F(x)^*F(x)) = \text{Tr}(F(y)^2) + \text{Tr}(F(z)^*F(z)) \geq \text{Tr}(y^2) + \text{Tr}(z^*z) = \text{Tr}(x^*x)$$

Réciproquement, si F a une norme triple inférieure à 1 et envoie les positifs sur les positifs alors, pour tout x, y positifs de norme inférieure à 1 on a d'une part :

$$\text{Tr}(\theta x \otimes y) = \text{Tr}(F(x)y) \geq 0$$

car $F(x) \geq 0, y \geq 0$, et d'autre part,

$$\text{Tr}(\theta x \otimes y) \leq \sqrt{\text{Tr}(F(x)^2)\text{Tr}(y^2)} \leq 1.$$

Conclusion :

★

Théorème 7 :

Soit $\theta \in \mathcal{L}(H_1 \otimes H_2)$ hermitien et $F = [\theta]$. L'opérateur θ appartient à $HS_{H_1} \otimes HS_{H_2}$ si et seulement si :

- pour tout opérateur positif x , $F(x)$ est positif,
- la norme triple de F relative à la norme associée au produit scalaire est inférieure à 1.

9.2 Normes L^p

Plus généralement, pour tout $p > 1$, et tout $x \in \mathcal{L}(H)$ hermitien, la matrice x se diagonalise en $\sum \lambda_i |\psi_i\rangle\langle\psi_i|$, avec $\lambda_i \in \mathbb{R}$. On pose alors $\|x\|_p = (\sum |\lambda_i|^p)^{\frac{1}{p}}$.

On en déduit une norme sur l'espace vectoriel réel $\mathcal{L}(H)$. En effet, tout $x \in \mathcal{L}(H)$ s'écrit $x = y + iz$, avec y et z hermitiens. (On choisit $y = \frac{1}{2}(x^* + x)$ et $z = \frac{1}{2i}(x - x^*)$.) Et on pose :

$$\|x\|_p := \|y\|_p + \|z\|_p.$$

Pour tout x, y positifs, il apparaît clair que $0 \leq Tr(x^*y) \leq \|x\|_p \|y\|_q$, avec $\frac{1}{p} + \frac{1}{q} = 1$.

En effet, on réécrit x et y sous la forme $x = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$ et $y = \sum \mu_j |\phi_j\rangle\langle\phi_j|$. On a alors :

$$Tr(xy) = \sum \lambda_i \mu_j |\langle\psi_i|\phi_j\rangle|^2 \geq 0$$

Or, d'après les inégalités de normes L_p , on a :

$$Tr(xy) \leq (\sum \lambda_i^p)^{1/p} (\sum_i (\sum_j \mu_j |\langle\psi_i|\phi_j\rangle|^2)^q)^{1/q}$$

Comme, $z \mapsto z^q$ est convexe et que $\sum_j |\langle\psi_i|\phi_j\rangle|^2 = 1$, on a :

$$(\sum_j \mu_j |\langle\psi_i|\phi_j\rangle|^2)^q \leq \sum_j \mu_j^q |\langle\psi_i|\phi_j\rangle|^2$$

donc

$$Tr(xy) \leq \|x\|_p (\sum_i \sum_j \mu_j^q |\langle\psi_i|\phi_j\rangle|^2)^{1/q}$$

On peut échanger l'ordre des sommes, et on obtient :

$$\begin{aligned} (\sum_i \sum_j \mu_j^q |\langle\psi_i|\phi_j\rangle|^2)^{1/q} &= (\sum_j \mu_j^q \sum_i |\langle\psi_i|\phi_j\rangle|^2)^{1/q} \\ &= (\sum_j \mu_j^q)^{1/q} = \|y\|_q \end{aligned}$$

d'où

$$0 \leq Tr(xy) \leq \|x\|_p \|y\|_q$$

La démonstration permet de voir d'une part que l'inégalité est vérifiée également par l'ensemble des hermitiens. Puis, en décomposant x et y quelconques en leurs parties hermitiennes et antihermitiennes, on obtient l'inégalité pour tout couple x, y .

Posons $E_p := \{x \geq 0 \mid \|x\|_p \leq 1\}$.

Lemme 9.4 :

| On a $\sim E_p = E_q$, avec $\frac{1}{p} + \frac{1}{q} = 1$.

Preuve : Soit $x \in E_p$. Pour tout $y \in E_q$, on a

$$0 \leq Tr(xy) \leq \|x\|_p \|y\|_q \leq 1,$$

donc $x \in \sim E_q$.

Réciproquement, si $x \in \sim E_q$ alors pour tout projecteur $|v\rangle\langle v|$, on a $|v\rangle\langle v| \in E_q$ donc $\langle v|x|v\rangle = Tr(x|v\rangle\langle v|) \geq 0$, donc x est positif. De plus,

$$\|x\|_p^p = \text{Tr}(x^p) = \text{Tr}(xx^{p-1}) = \|x^{p-1}\|_q \text{Tr}\left(x \frac{x^{p-1}}{\|x^{p-1}\|_q}\right) \leq \|x^{p-1}\|_q.$$

En effet, $\frac{x^{p-1}}{\|x^{p-1}\|_q}$ appartient à E_q donc $\text{Tr}\left(x \frac{x^{p-1}}{\|x^{p-1}\|_q}\right) \leq 1$.

Or,

$$\|x^{p-1}\|_q = (\text{Tr}(x^{q(p-1)}))^{1/q} = (\text{Tr}(x^p))^{p/(pq)} = \|x\|_p^{p-1}$$

car $q(p-1) = \frac{p-1}{1-\frac{1}{p}} = \frac{p-1}{\frac{p-1}{p}} = p$ et $\frac{p}{q} = p(1 - \frac{1}{p}) = p-1$. On en déduit que $\|x\|_p^p \leq \|x\|_p^{p-1}$ ce qui équivaut à $\|x\|_p \leq 1$.

On a bien $x \in E_p$. ★

On dispose donc de nouveaux espaces cohérents quantiques, le lemme impliquant que tous les E_q sont des ECQs.

Par de deux E_q

Soit H_1 et H_2 deux espaces de Hilbert de dimension finie et p, q deux réels strictement supérieurs à 1. On note p' le réel conjugué de p c'est-à-dire celui vérifiant : $\frac{1}{p} + \frac{1}{p'} = 1$.

On s'intéresse à l'espace cohérent : $E := E_p^1 \otimes E_q^2 = E_{p'}^1 \otimes E_q^2$ les indices 1 et 2 se référant à l'espace de Hilbert considéré.

Lemme 9.5 :

Soit $\theta \in E$ et $F = [\theta]$. Alors F envoie les positifs sur les positifs et sa norme triple relative aux normes $\|\cdot\|_{p'}$ et $\|\cdot\|_q$ est inférieure à 1.

Preuve : La preuve est presque la même que pour les Hilbert-Schmidt.

1^{er} cas : $x = 0$. On a $F(x) = 0$.

2^{ème} cas : $x > 0$. On pose $x' = \frac{x}{\|x\|_{p'}}$. On a $\|x'\|_{p'} = 1$ donc $x' \in E_{p'}^1$, donc $F(x') \in E_q^2$,

c'est-à-dire $\frac{\|F(x)\|_q}{\|x\|_{q'}} = \left\| \frac{F(x)}{\|x\|_{q'}} \right\|_q = \|F(x')\|_q \in [0, 1]$, on a bien $\|F(x)\|_q \leq \|x\|_{p'}$.

3^{ème} cas : x hermitien. L'opérateur x se diagonalise, il se met donc sous la forme $x = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$. On pose alors $x^+ = \sum |\lambda_i| |\psi_i\rangle\langle\psi_i|$. On a $\|x\|_{p'} = \|x^+\|_{p'}$. De plus,

$$F(x) = \sum \lambda_i F(|\psi_i\rangle\langle\psi_i|)$$

Or, F envoie les positifs sur les positifs donc pour tout i , $F(|\psi_i\rangle\langle\psi_i|) \geq 0$, en notant $|v_j\rangle$ une base de diagonalisation de $F(x)$, on a :

$$\|F(x)\|_q^q = \sum_j \left| \sum_i \lambda_i \langle v_j | F(|\psi_i\rangle\langle\psi_i|) | v_j \rangle \right|^q$$

$$\|F(x)\|_q^q \leq \sum_j \left(\sum_i |\lambda_i| \langle v_j | F(|\psi_i\rangle\langle\psi_i|) | v_j \rangle \right)^q = \sum_j \langle v_j | F(x^+) | v_j \rangle^q$$

car $z \mapsto z^q$ est croissante et $F(|\psi_i\rangle\langle\psi_i|)$ est positif pour tout i .

En notant $|w_i\rangle_i$ une base de diagonalisation de $F(x^+)$ associée aux valeurs propres μ_i , on a :

$$\|F(x)\|_q^q \leq \sum_j \left(\sum_i \mu_i |\langle w_i | v_j \rangle|^2 \right)^q$$

Or, $z \mapsto z^q$ est convexe et $\sum_i |\langle w_i | v_j \rangle|^2 = 1$ donc

$$\left(\sum_i \mu_i |\langle w_i | v_j \rangle|^2 \right)^q \leq \sum_i |\langle w_i | v_j \rangle|^2 \mu_i^q$$

$$\|F(x)\|_q^q \leq \sum_i \mu_i^q \sum_j |\langle w_i | v_j \rangle|^2 = \sum_i \mu_i^q = \|F(x^+)\|_q^q$$

Finalement,

$$\|F(x)\|_q \leq \|F(x^+)\|_q \leq \|x^+\|_{p'} = \|x\|_{p'}.$$

Denier cas : x quelconque.

x se décompose en une partie hermitienne et une partie anti-hermitienne :

$$x = y + iz$$

On a $F(x) = F(y) + iF(z)$ donc $F(y)$ est la partie hermitienne de $F(x)$ et $F(z)$ la partie antihermitienne, on en déduit :

$$\|F(x)\|_q = \|F(y)\|_q + \|F(z)\|_q \leq \|y\|_{p'} + \|z\|_{p'} = \|x\|_{p'}.$$

Réciproquement, si la norme triple de F est inférieure à 1 et que F envoie les positifs sur les positifs alors θ est dans E .

En effet, pour tout x, y positifs tels que $\|x\|_{p'} \leq 1$ et $\|y\|_{q'} \leq 1$, on a

$$0 \leq \text{Tr}(\theta x \otimes y) = \text{Tr}(F(x)y) \leq \|F(x)\|_q \|y\|_{q'} \leq \|x\|_{p'} \leq 1$$

★

Conclusion :

Théorème 8 :

- Soit $\theta \in \mathcal{L}(H_1 \otimes H_2)$ hermitien et $F = [\theta]$, θ appartient à $E = E_p \otimes E_q$ si et seulement si :
- pour tout projecteur $|v\rangle\langle v|$, $F(|v\rangle\langle v|)$ est positif,
 - la norme triple de F relative à $\|\cdot\|_{p'}$ et $\|\cdot\|_q$ est inférieure ou égale à 1.

10 Autour de la positivité

On va s'intéresser de plus près aux questions de positivité qui se posent dans le modèle des ECQ. Pour cela on se basera sur un article de P. Selinger [15]. L'objet de départ de cet article est de proposer une façon de décrire l'algorithmique quantique avec un langage "haut niveau", par opposition avec l'approche habituelle, très proche de la machine (le plus souvent, on revient au niveau des portes quantiques de base).

Après avoir présenté la syntaxe de son langage, l'auteur en donne une sémantique basée sur une catégorie dont les objets sont des produits cartésiens d'ensembles de matrices densité et les morphismes des opérateurs superpositifs.

Cette construction est une des sources d'inspiration pour les ECQ. Pourtant il y a une différence qui saute aux yeux si on regarde ces deux modèles (du calcul quantique et du fragment parfait de la logique linéaire respectivement) : alors que P. Selinger utilise des opérateurs de densité (positifs) et des transformations superpositives, J.-Y. Girard n'impose comme restriction aux opérateurs que d'être hermitiens et les morphismes considérés dans le cas des ECQ sont *toutes* les applications linéaires.

La discussion qui suit va essayer d'éclairer les questions qui se posent autour de cette différence.

10.1 De l'isomorphisme à la dualité

En 7.2, on a décrit un isomorphisme entre $\mathcal{H}(H_1) \rightarrow \mathcal{H}(H_2)$ et $\mathcal{H}(H_1 \otimes H_2)$, plutôt comme un préliminaire technique permettant d'énoncer des résultats comme le théorème 3.

En réalité, le choix de cet isomorphisme n'est pas indépendant du reste de la construction. On va même voir qu'il y a en quelque sorte une correspondance entre ce choix et celui de la relation de polarité, et qu'on aurait pu commencer par donner l'isomorphisme pour en déduire la définition de " \sim ".

Négation et implication

Dans un modèle de la logique linéaire où l'on peut interpréter à la fois la négation, l'implication linéaire et les éléments neutres (en particulier \perp), on doit avoir certains isomorphismes. En particulier :

$$\sim A \simeq A \rightarrow \perp$$

car la preuve de l'équivalence entre les deux formules est essentiellement une identité.

Ceci constitue une première étape : si on a un élément neutre pour le \wp et une implication linéaire, on peut en déduire une négation.

Implication et isomorphisme

Poursuivons le raisonnement : si un modèle admet un isomorphisme entre "les morphismes de A dans B " (dans le cas des espaces cohérents, $A \rightarrow B$) et un autre objet du modèle, on peut raisonnablement appeler cet objet $A \rightarrow B$ puis voir si cette définition est cohérente avec le reste du modèle.

Conclusion

Mettons tout ça ensemble. Pour construire les ECQ on aurait pu¹⁰ partir d'une définition n'utilisant pas la négation, par exemple "vérifier les hypothèses du théorème du Bipolaire", puis définir un objet dualisant \perp et utiliser l'isomorphisme pour définir une implication linéaire, puis une négation. De ce point de vue, on comprend que le choix (il n'en existe pas qu'un seul!) de l'isomorphisme entre $\mathcal{H}(H_1) \rightarrow \mathcal{H}(H_2)$ et $\mathcal{H}(H_1 \otimes H_2)$ est déterminant pour la construction du modèle.

¹⁰Théoriquement en tout cas. Sortir les hypothèses du théorème du Bipolaire "de nulle part" relève plutôt de la science-fiction.

10.2 L'isomorphisme de Selinger

Dans le but de rester le plus proche possible de ce qui apparaît en informatique quantique, P Selinger prend directement comme objet de base des ensembles¹¹ de matrices densité sur des espaces de différentes dimensions.

Dans ce modèle, on a comme pour les ECQ un isomorphisme entre les applications linéaires de $\mathbf{M}_m(\mathbb{C})$ vers $\mathbf{M}_n(\mathbb{C})$ et $\mathbf{M}_{mn}(\mathbb{C})$. Moyennant le choix d'une base, cet isomorphisme sur les matrices donne un isomorphisme sur les opérateurs.

On le définit de la façon suivante :

Définition 10.1 : χ

On note $E_{i,j}$ la matrice dont seul le coefficient en position i, j est non nul et vaut 1.

Pour $F \in \mathbf{M}_m(\mathbb{C}) \rightarrow \mathbf{M}_n(\mathbb{C})$ on définit la matrice caractéristique de F , par blocs :

$$\chi_F := \begin{pmatrix} F(E_{1,1}) & \dots & F(E_{1,n}) \\ \vdots & \ddots & \vdots \\ F(E_{n,1}) & \dots & F(E_{n,n}) \end{pmatrix}$$

Proposition 10.2 : $\mathbf{M}_m(\mathbb{C}) \rightarrow \mathbf{M}_n(\mathbb{C}) \simeq \mathbf{M}_{mn}(\mathbb{C})$

|| χ est un est un isomorphisme entre les espaces $\mathbf{M}_m(\mathbb{C}) \rightarrow \mathbf{M}_n(\mathbb{C})$ et $\mathbf{M}_{mn}(\mathbb{C})$.

Preuve : χ est injective car $\chi_F = 0$ impose que $F(E_{i,j}) = 0$ pour tout i, j et donc $F = 0$, les $E_{i,j}$ formant une base de $\mathbf{M}_m(\mathbb{C})$.

Pour la surjectivité, il suffit de découper la matrice en blocs carrés de taille n et de poser $F(E_{i,j})$ égal au contenu du bloc correspondant. ★

L'isomorphisme χ possède une propriété analogue à la proposition 7.2 :

Proposition 10.3 :

|| Soit $F \in \mathbf{M}_m(\mathbb{C}) \rightarrow \mathbf{M}_n(\mathbb{C})$. On a
 || pour tous $X \in \mathbf{M}_m(\mathbb{C})$ et $Y \in \mathbf{M}_n(\mathbb{C})$: $Tr(\chi_F \cdot {}^tX \otimes Y) = Tr(F(X).Y)$

Preuve : on commence par remarquer que

$$\chi_F = \sum_{i,j} E_{i,j} \otimes F(E_{i,j}). \text{ On a donc } Tr(\chi_F \cdot {}^tX \otimes Y) = \sum_{i,j} Tr(E_{i,j} {}^tX) \cdot Tr(F(E_{i,j})Y)$$

Mais $Tr(E_{i,j} {}^tX)$ est égal à $({}^tX)_{j,i}$, le coefficient en position (i, j) de tX , c'est à dire $X_{i,j}$.
 On a donc

$$Tr(\chi_F \cdot {}^tX \otimes Y) = \sum_{i,j} Tr(X_{i,j} F(E_{i,j}).Y) = Tr(F(X).Y)$$

★

¹¹Des produits cartésiens de tels ensembles, en réalité, mais on se contentera du cas simple où le produit est réduit à un seul élément.

10.2.1 Superpositivité

La raison pour laquelle Selinger préfère utiliser l'isomorphisme χ est qu'il possède une propriété intéressante que θ n'a pas : χ fournit un critère de superpositivité.

Théorème 9 : χ et superpositivité

- χ_F est pure si et seulement si F est de la forme $M \rightarrow AMA^\dagger$ pour $A \in \mathbf{M}_{m,n}(\mathbb{C})$.
- Les trois propriétés suivantes sont équivalentes :
 1. F est superpositive
 2. χ_F est positive
 3. F peut s'écrire comme une somme finie de transformations de la forme $M \rightarrow AMA^\dagger$

Preuve : pour la première propriété, on remarque que si $\chi_F = UU^\dagger$ pour $U \in \mathbb{C}^{mn}$, on peut découper U en m vecteurs de \mathbb{C}^n de la façon suivante :

$$U = \begin{pmatrix} U_1 \\ \vdots \\ U_m \end{pmatrix}$$

puis on définit par blocs $A := (U_1 \ U_2 \ \dots \ U_m)$ et on a alors $F(E_{i,j}) = U_i U_j^\dagger$ par définition de χ , enfin comme $U_i U_j = AE_{i,j}A^\dagger$ pour tous i, j on a bien $F : M \rightarrow AMA^\dagger$.

Réciproquement, si $F : M \rightarrow AMA^\dagger$ on peut faire marcher la construction en sens inverse pour obtenir un U tel que $\chi_F = UU^\dagger$.

Pour la deuxième partie du théorème, commençons par **1. implique 2.** : on définit par blocs la matrice

$$E := \begin{pmatrix} E_{1,1} & \dots & E_{1,n} \\ \vdots & \ddots & \vdots \\ E_{n,1} & \dots & E_{n,n} \end{pmatrix}$$

et on remarque que $\chi_F = (Id \otimes F)(E)$ et que la matrice E est positive.

Donc, si F est superpositive, $(Id \otimes F)(E)$ doit être positive.

Pour **2. implique 3.**, supposons χ_F positive et décomposons la en une somme de matrices pures, $\chi_F = B_1 + \dots + B_k$. D'après la première partie du théorème, chaque B_i correspond à une transformation $F_i : M \rightarrow A_i M A_i^\dagger$. Par linéarité de χ , on a $F = F_1 + \dots + F_k$, c'est à dire **3.**

Enfin, **3. implique 1.** : soit F de la forme $M \rightarrow A^\dagger M A$ (comme une somme d'applications superpositives est superpositive, on en déduit le cas "somme finie").

Soit $B \in \mathbf{M}_{km}^+(\mathbb{C})$, décomposons B comme somme de produits tensoriels de matrices de $\mathbf{M}_k^+(\mathbb{C})$ et $\mathbf{M}_m^+(\mathbb{C})$: $B = \sum_i M_i \otimes N_i$. On a alors $(Id_{\mathbf{M}_k^+(\mathbb{C})} \otimes F)(B) = \sum_i M_i \otimes A N_i A^\dagger$.

Soit alors $U \otimes V \in \mathbf{M}_{k,1}(\mathbb{C}) \otimes \mathbf{M}_{m,1}(\mathbb{C})$. On a

$$\begin{aligned} (U^\dagger \otimes V^\dagger) (Id_{\mathbf{M}_k^+(\mathbb{C})} \otimes F)(B) (U \otimes V) &= \sum_i U^\dagger M_i U \otimes V^\dagger A^\dagger N_i A V \\ &= (U^\dagger \otimes (AV)^\dagger) B (U \otimes AV) \geq 0 \quad \text{car } B \text{ est positive.} \end{aligned}$$

Donc $(Id_{\mathbf{M}_k^+(\mathbb{C})} \otimes F)(B)$ est positive, ceci valant pour toute matrice B positive, $Id_{\mathbf{M}_k^+(\mathbb{C})} \otimes F$ est bien superpositive. ★

10.3 Ce qui change avec les ECQ, conséquences

Il y a de bonnes raisons de ne pas vouloir utiliser le modèle de Selinger en l'état. La principale étant, comme on l'a vu dans la partie précédente que l'isomorphisme χ force à choisir une base, ce qui est une forme de subjectivité avant l'heure (avant d'effectuer une mesure). Cela semble aller à l'encontre des principes de base de la mécanique quantique, mais cela a un sens en informatique quantique, ou l'on fait de toutes façons des calculs par rapport à une base privilégiée, fixée à l'avance.

Mais c'est moins évident en logique, l'idée du modèle étant de passer d'une interprétation de la logique comme "actions" sur des ressources à une interprétation comme "actions quantiques" sur des ressources quantiques, et donc d'essayer de faire correspondre aux formules de logique des objets et des transformations quantiques dans toute leur généralité. Construire un modèle en se basant sur l'isomorphisme χ implique d'avoir une relation de polarité dépendante de la base, ce qui n'est pas très satisfaisant.

Ces remarques conduisent naturellement à préférer l'isomorphisme décrit dans la section 7.2 au χ de Selinger. Ce choix a d'importantes conséquences sur ce qui nous intéresse ici : les questions de positivité.

Le problème vient du fait que l'isomorphisme θ ne "voit pas" les opérateurs positifs, contrairement à χ qui vérifie le théorème 9. On peut le voir sur un exemple :

Prenons le cas des booléens quantiques P_H et de l'espace $P_H \multimap P_H \simeq P_H \rightarrow P_H$. Ce dernier doit forcément contenir l'application identique, et on a vu que $\theta_{Id} = \sigma$, le *twist*, qui est une réflexion et donc n'est pas positive.

On est donc dans la situation suivante : les booléens quantiques forment un ECQ d'opérateurs positifs, mais la remarque précédente interdit de se limiter, comme chez Selinger, à des opérateurs positifs dans tous les cas, sous peine de ne pas avoir l'identité dans $P_H \multimap P_H$.

On peut par ailleurs remarquer que $P_H \multimap P_H$ correspond à *tous* les opérateurs préservant P_H , c'est à dire les opérateurs *positifs* et préservant la trace. On a vu que cette classe contenait plus que les superopérateurs, ce qui signifie que le modèle des ECQ accepte comme transformations de l'ECQ engendré par les matrices densité des transformations qui n'ont **pas de sens physique**.

10.4 Réconcilier les deux approches ?

On va essayer maintenant d'exploiter les remarques précédentes pour jeter les bases d'une construction un peu différente des ECQ, qui sera détaillée dans la section suivante. Notre but va être de profiter du "meilleur des deux mondes" : la positivité du modèle de P. Selinger et l'indépendance par rapport à la base de celui de J.-Y. Girard.

Le point de départ est une remarque de quelques lignes dans l'article [15] sur l'isomorphisme χ . L'auteur y explique qu'on peut en fait le rendre indépendant de la base à condition de le considérer comme un isomorphisme entre $\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$ et $\mathcal{L}(H_1^* \otimes H_2)$, que l'on transforme ensuite *via* le choix d'une base (qui permet de définir un isomorphisme entre H_1 et H_1^*) en un isomorphisme entre $\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$ et $\mathcal{L}(H_1 \otimes H_2)$. On va donc essayer de reconstruire un modèle utilisant cet isomorphisme.

La deuxième idée est que, si H_1 et H_1^* ne sont pas canoniquement isomorphes¹², c'est par contre le cas de $\mathcal{L}(H_1)$ et $\mathcal{L}(H_1^*)$, grâce à l'isomorphisme suivant :

Définition 10.4 : transposée

Si H_1 est un espace de Hilbert de dimension finie et $f \in \mathcal{L}(H_1)$, on définit la *transposée* de f , notée ${}^t f$ par :

$$\text{Pour tout } \varphi \in H_1^*, \quad {}^t f(\varphi) := \varphi \circ f$$

¹²Il sont "canoniquement anti-isomorphes" à cause de problèmes de C-linéarité.

Proposition 10.5 : $\mathcal{L}(H_1) \simeq \mathcal{L}(H_1^*)$

|| Soit H_1 un espace de Hilbert de dimension finie. La transposée définit un isomorphisme entre $\mathcal{L}(H_1)$ et $\mathcal{L}(H_1^*)$.

Preuve : l'injectivité est immédiate, car ${}^t f = 0$ implique que pour tout φ , $\varphi \circ f = 0$ ce qui est impossible s'il existe x tel que $f(x) \neq 0$.

La surjectivité en découle en dimension finie, mais on peut également utiliser l'argument suivant : H_1 étant un espace de Hilbert, on peut identifier H_1 et H_1^{**} en identifiant $x \in H_1$ et la forme linéaire sur H_1^* qui à tout φ associe $\varphi(x)$, que l'on notera \tilde{x} .

On a alors ${}^{tt} f(\tilde{x}) = \tilde{x} \circ {}^t f$, puis pour tout $\varphi \in H_1^*$: $\tilde{x} \circ {}^t f(\varphi) = \tilde{x}(\varphi \circ {}^t f) = \varphi(f(x))$. C'est à dire ${}^{tt} f(\tilde{x}) = \widetilde{f(x)}$, et donc à l'identification $H_1 \simeq H_1^{**}$ près, ${}^{tt} f = f$.

La transposée est involutive et injective, c'est donc une bijection. ★

Forts de ce nouvel outil, revenons sur un point que l'on a totalement passé sous silence lors de la définition des ECQ.

Après avoir défini la polarité \perp , on a pu définir la négation $\sim X$ de l'espace X . On commence pour cela par définir sa trame, $|\sim X| := |X|$. Derrière cette définition se cache soit une identification de $|X|$ et $|X|^*$ (et donc le choix d'une base), soit une obligation d'utiliser l'isomorphisme θ plutôt que χ puisque l'on veut bien un isomorphisme entre $\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$ et $\mathcal{L}(H_1 \otimes H_2)$ (et pas $\mathcal{L}(H_1^* \otimes H_2)$).

Avec la transposée, on peut définir une relation de polarité mettant en jeu des éléments de $\mathcal{H}(H_1)$ et de $\mathcal{H}(H_1^*)$:

Définition alternative de la polarité :

Si H_1 est un espace de Hilbert de dimension finie et f, g sont respectivement dans $\mathcal{H}(H_1)$ et $\mathcal{H}(H_1^*)$, on dira que f et g sont *polaires*, noté $f \perp^+ g$, si :

$$Tr({}^t f g) = Tr(f {}^t g) \in [0, 1]$$

On peut à partir de là définir $\sim X$ de trame $|X|^*$, et redéfinir à partir de là les différentes notions qui apparaissent avec les ECQ. On utilisera bien sûr l'isomorphisme χ à la place de θ , ce qui permettra de se restreindre aux opérateurs positifs sans perdre l'identité, car Id étant superpositive, χ_{Id} est positive par le théorème 9.

Avant de poser les définitions, voyons quelques propriétés de la transposée, utiles pour la suite.

Lemme 10.6 : représentation matricielle et transposée

|| Soit $B := (|e_1\rangle, \dots, |e_n\rangle)$ une base de l'espace de Hilbert H_1 et notons $B^* := (\langle e_1|, \dots, \langle e_n|)$ la base duale de H_1^* .

Alors, si $h \in \mathcal{H}(H_1)$ est représenté par la matrice A dans la base B , ${}^t h$ est représenté par ${}^t A$ (la matrice transposée de A) dans la base B^* .

Preuve : posons C la matrice représentant ${}^t h$ dans B^* .

Pour toute matrice M , on notera $M_{i,j}$ le coefficient en position (i, j) de M .

On a :

$$\begin{aligned} C_{i,j} &= \text{composante sur } \langle e_j| \text{ de } {}^t h(\langle e_i|) = \text{composante sur } \langle e_j| \text{ de } \langle e_i| \circ h \\ &= \langle e_i| \circ h(|e_j\rangle) = \text{composante sur } |e_i\rangle \text{ de } h(|e_j\rangle) = A_{j,i} \end{aligned}$$

Ce qui prouve bien que $C = {}^t A$. ★

Corollaire 10.7 :

1. La transposée d'un opérateur positif est positive.
2. La transposée préserve la norme des opérateurs.
3. La transposée préserve la trace des opérateurs

Preuve : immédiat avec le lemme, la transposée d'une matrice positive est positive et a la même norme et la même trace. ★

11 Espaces Cohérents Positifs

On utilise la notion de polarité vue en 10.4, ce qui permet de définir le polaire d'un ensemble d'opérateurs positifs.

Définition 11.1 : polaire positif

Si $X \subseteq \mathcal{H}^+(|X|)$ —l'ensemble des hermitiens positifs sur $|X|$ — on définit le *polaire positif* de X par :

$$\sim^+ X := \{ h \in \mathcal{H}^+(|X|^*) \mid \forall g \in X, g \perp^+ h \}$$

S'ensuit la définition des espaces cohérents positifs :

Définition 11.2 : espace cohérent positif

On appellera *espace cohérent positif* (ECQ⁺) de trame $|X|$ tout sous-ensemble de $\mathcal{H}^+(|X|)$ égal à son bipolaire positif.

Cette nouvelle dualité vérifie les mêmes propriétés de base que \sim , à savoir :

Lemme 11.3 :

1. La polarité positive est décroissante pour l'inclusion : $X \subseteq Y$ implique $\sim^+ Y \subseteq \sim^+ X$.
2. La bipolarité positive est donc croissante pour l'inclusion.
3. La polarité positive échange union et intersection : $\sim^+(X \cup Y) = \sim^+ X \cap \sim^+ Y$.
4. Pour tout X , $X \subseteq \sim^+ \sim^+ X$.
5. Pour tout X , $\sim^+ X$ est un ECQ⁺ : $\sim^+ \sim^+ \sim^+ X = \sim^+ X$.

11.1 Le théorème du Bipolaire

On va montrer ici la version ECQ⁺ du théorème du Bipolaire.

Par rapport à la version ECQ, on est confronté à un nouveau problème : l'ensemble des opérateurs positifs n'est pas un espace vectoriel. Cela complique l'utilisation du théorème de hahn-Banach car rien ne garantit que la forme linéaire obtenue corresponde à un opérateur positif.

On contourne le problème en utilisant un théorème un peu moins général que le théorème de Hahn-Banach, mais également plus précis : le théorème de projection sur un convexe.

On montre donc le théorème suivant :

Théorème du Bipolaire positif :

$X \subseteq \mathcal{H}^+(|X|)$ est un ECQ⁺ si et seulement si :

1. X est non-vidé.
2. X est convexe et fermé
3. Si $x \in X$ et $y \leq x$, alors $y \in X$.

Rappelons l'énoncé du théorème de projection sur un convexe dans un espace de Hilbert.

Théorème de projection sur un convexe :

Si C est un convexe fermé d'un espace de Hilbert, il existe une unique application p_C avec la propriété suivante :

$$\text{pour tout } z \in C, (z - p_C(x)|x - p_C(x)) \leq 0$$

On appelle cette application *projection orthogonale* sur le convexe C .

De plus, pour tout x , le projeté $p_C(x)$ est le point de X à distance minimale de x .

Ce théorème implique le théorème de Hahn-Banach (version géométrique) dans le cas particulier des espaces de Hilbert. Dans notre cas, il présente l'avantage de donner plus d'informations sur la forme linéaire obtenue par l'axiome du choix dans le cas général.

On aura également besoin du lemme suivant :

Lemme 11.4 :

Soient x et y des opérateurs positifs d'un espace de Hilbert U de dimension finie. Si $x - y \geq 0$, alors $\|x - y\|_2 \leq \|x\|_2$

Preuve :

$$\|x - y\|_2^2 = Tr((x - y)^2) = Tr(x^2) + Tr(y^2) - 2Tr(xy) = \|x\|_2^2 - Tr((x - y)y) - Tr(xy)$$

Or, x et y sont positifs, donc $Tr(xy) \geq 0$ et $x - y$ est positif donc $Tr((x - y)y) \geq 0$. On a bien $\|x - y\|_2^2 \leq \|x\|_2^2$ et donc $\|x - y\|_2 \leq \|x\|_2$.



Preuve du théorème : Soit X un ECQ⁺. Montrons que X vérifie 1.-3.. On pose $Y = \sim^+ X$.

On a $X = \sim^+ \sim^+ X = \sim^+ Y$.

1. L'opérateur nul est positif et vérifie pour tout $y \in Y$, $Tr({}^t y 0) = Tr(0) = 0 \in [0, 1]$, donc $0 \in X$.
2. Soit $x_1, x_2 \in X$ et $t \in [0, 1]$. Montrons que $x = tx_1 + (1 - t)x_2$ appartient à X . Tout d'abord x est positif comme somme de deux opérateurs positifs, de plus, soit $y \in Y$, on a $Tr({}^t y x) = tTr({}^t y x_1) + (1 - t)Tr({}^t y x_2) \in [0, 1]$. Donc X est convexe. De plus, X est l'intersection de l'ensemble des opérateurs positifs (fermé) avec les images réciproques par les applications continues $x \mapsto Tr({}^t y x)$ pour tout $y \in Y$ de $[0, 1]$ (fermé), c'est donc également un fermé.
3. Soit $x \in X$ et $0 \leq z \leq x$. Montrons que z appartient à X . Soit $y \in Y$. Comme z est positif, $Tr({}^t y z) \geq 0$, et comme $x - z$ l'est également, $Tr({}^t y z) = Tr({}^t y x) - Tr({}^t y (x - z)) \leq Tr({}^t y x) \leq 1$.

Montrons l'implication réciproque. Soit X vérifiant 1.-3.. Soit $x \notin X$, positif. On va montrer que $x \notin \sim^+ \sim^+ X$.

Posons $y = p_X(x)$ la projection de x sur le convexe fermé X , et $z = x - y$. On veut montrer que z est positif. Pour cela, on décompose z en $z = z_+ + z_-$, avec $z_+ \geq 0$, $z_- \leq 0$ et $z_+ z_- = z_- z_+ = 0$, puis on montre que z_- est nul.

On note P la projection orthogonale sur $\text{Im}(y)y$ et $z'_- = Pz_-P$. Montrons que z'_- est nul.

L'image de z'_- est incluse dans celle de y donc il existe $\lambda_1 > 0$ tel que pour tout $0 \leq \lambda \leq \lambda_1$ l'opérateur $y + \lambda z'_-$ soit positif : sur $\text{Im}(y)$, y n'a que des valeurs propres strictement positives et donc y est dans l'intérieur de $\mathcal{H}^+(\text{Im}(y))$. Il existe donc une boule ouverte de centre y incluse dans $\mathcal{H}^+(\text{Im}(y))$. Notons r son rayon : $\frac{r}{\|z'_-\|}$ fournit un λ_1 . En effet, pour tout $0 \leq \lambda \leq \frac{r}{\|z'_-\|}$, $y + \lambda z'_-$ est à une distance inférieure à r de y et est donc positif.

De même, l'image de z'_- est incluse dans celle de z_- donc il existe $\lambda_2 > 0$ tel que pour tout $\lambda \leq \lambda_2$, l'opérateur $z_- - \lambda z'_-$ soit négatif.

Posons $\lambda = \min(\lambda_1, \lambda_2) > 0$, $y + \lambda z'_-$ est positif et inférieur à $y \in X$ donc $y + \lambda z'_- \in X$, de plus, on a :

$$\|x - (y + \lambda z'_-)\|_2^2 = \|z_+ + (z_- + \lambda z'_-)\|_2^2$$

Or, $z_+ z_- = 0$ et $z_+ z'_- = 0$ donc

$$\|x - (y + \lambda z'_-)\|_2^2 = \|z_+\|_2^2 + \|z_- - \lambda z'_-\|_2^2$$

D'après le lemme appliqué à $-\lambda z'_-$ et $-z_-$, on a $\|z_- + \lambda z'_-\|_2^2 \leq \|z_-\|_2^2$ donc

$$\|x - (y + \lambda z'_-)\|_2^2 \leq \|z_+\|_2^2 + \|z_-\|_2^2 = \|z_+ + z_-\|_2^2 = \|x - y\|_2^2$$

Comme y est la projection sur le convexe X , par unicité de p_X , on a $\lambda z'_- = 0$ et comme $\lambda > 0$, $z'_- = 0$.

On en déduit que z_- est également nul. Comme $z'_- = 0$, on a $\text{Im}(z_-) \subseteq \text{Ker}(y)$. De plus, par définition, $\text{Im}(z_-) \subseteq \text{Ker}(z_+)$. Soit alors $|v\rangle \in \text{Im}(z_-)$, on a $0 \leq \langle v|x|v\rangle = \langle v|z_-|v\rangle \leq 0$, d'où $\langle v|z_-|v\rangle = 0$ pour tout vecteur $|v\rangle$. On a bien $z_- = 0$, et donc $z = z_+ \geq 0$.

Soit $\varepsilon = \|z\|_2^2$. ε est strictement positif puisque $x \notin X$. On pose $M = \langle y|z\rangle + \frac{\varepsilon}{2} > 0$ et $z' = \frac{z}{M}$. Montrons que $z' \in \sim^+ X$. En effet, pour tout $x_0 \in X$, on a :

$$\text{Tr}(x_0 {}^t z') = \text{Tr}(x_0 \frac{z}{M}) = \frac{\text{Tr}(x_0(x - p_X(x)))}{M}$$

Or, d'après le théorème de projection sur un convexe :

$$\text{Tr}(x_0(x - y)) = \text{Tr}((x_0 - y)(x - y) + y(x - y)) \leq \text{Tr}(yz) \leq M.$$

donc $\text{Tr}(x_0 {}^t z') \leq 1$. De plus, $z' \geq 0$ donc $z' \in \sim^+ X$. Enfin, $\text{Tr}(x {}^t z') = \frac{\text{Tr}((y+z)z)}{M} = \frac{M+\varepsilon/2}{M} > 1$ donc x n'appartient pas au bipolaire de X , ce qui achève la démonstration. ★

11.2 L'isomorphisme dans le cas positif

On va adapter l'isomorphisme χ (initialement isomorphisme entre espaces de matrices) à notre cadre.

(dans ce qui suit, H_1 et H_2 sont des espaces de Hilbert de dimension finie.)

Théorème 10 : $\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2) \simeq \mathcal{L}(H_1^* \otimes H_2)$

L'espace des applications linéaires de $\mathcal{L}(H_1)$ dans $\mathcal{L}(H_2)$ est isomorphe à celui des opérateurs de $H_1^* \otimes H_2$

On notera provisoirement cet isomorphisme ζ .

Preuve : similaire au théorème 2, on utilise toujours l'identification 7.1 et la commutativité à isomorphisme près du produit tensoriel ★

En réalité, ζ n'est rien d'autre que la version indépendante de la base de χ , au sens suivant :

Proposition 11.5 :

Soit $B := (|e_1\rangle, \dots, |e_n\rangle)$ une base de H_1 et $C := (|f_1\rangle, \dots, |f_n\rangle)$ une base de H_1 . On note $B^* := (\langle e_1|, \dots, \langle e_n|)$ la base duale de H_1^* .
 Soit $F \in \mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$. On note F' l'application sur les matrices induite par F en passant par les représentations dans les bases B et C .
 Alors, $\zeta(F)$ correspond dans la base $B^* \otimes C$ à la matrice $\chi_{F'}$.

Preuve :

On montre le résultat pour les $F_{i,j,k,l}$ qui envoient $|e_i\rangle\langle e_j|$ sur $|f_k\rangle\langle f_l|$ et les autres projecteurs $|e_{i'}\rangle\langle e_{j'}|$ sur 0. On en déduira le résultat par linéarité, les $F_{i,j,k,l}$ formant une base de $\mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$.

Du point de vue de l'identification 7.1, $F_{i,j,k,l}$ correspond au vecteur $|f_k\rangle \otimes \langle f_l| \otimes \langle e_i| \otimes |e_j\rangle$. On a donc $\zeta(F_{i,j,k,l}) = \langle e_i| \otimes |f_k\rangle \otimes |e_j\rangle \otimes \langle f_l|$, ce qui correspond dans la base $B^* \otimes C$ à la matrice avec 1 en position $(i, k), (j, l)$ et 0 partout ailleurs.

Ensuite, comme $\chi'_F = \begin{pmatrix} F'(E'_{1,1}) & \dots & F'(E'_{1,n}) \\ \vdots & \ddots & \vdots \\ F'(E'_{n,1}) & \dots & F'(E'_{n,n}) \end{pmatrix} = E_{i,j} \otimes E_{k,l}$, c'est à dire la matrice avec des 0 partout et 1 en position $(i, k), (j, l)$, on a bien le résultat. ★

Pour cette raison, on identifiera les deux isomorphismes et on notera χ_F au lieu de $\zeta(F)$. De plus, l'inverse de χ sera noté $\langle \cdot \rangle$.

Corollaire 11.6 : $\mathcal{H}^+(H_1) \rightarrow^+ \mathcal{H}^+(H_2) \simeq \mathcal{H}^+(H_1^* \otimes H_2)$

| Soit $F \in \mathcal{L}(H_1) \rightarrow \mathcal{L}(H_2)$, χ_F est positive si et seulement si F est superpositive.

Preuve : grace à la proposition 11.5, on peut appliquer le théorème 9. ★

C'est cette propriété qui nous intéresse pour les ECQ⁺, mais le théorème 9 est bien sûr toujours valide.

Enfin, on a une propriété reliant la trace et l'isomorphisme qui nous sera utile pour certains calculs.

Corollaire 11.7 :

Pour tout $\phi \in \mathcal{L}(H_1^* \otimes H_2)$ on a :

$$\text{Pour tous } x \in \mathcal{L}(H_1^*) \text{ et } y \in \mathcal{L}(H_2), \text{Tr}(\phi.(x \otimes y)) = \text{Tr}(\langle \phi \rangle(x).y)$$

Preuve : là encore, la proposition 11.5 permet d'appliquer la proposition 10.3. ★

11.3 Les connecteurs positifs

On peut maintenant donner une nouvelle définition des connecteurs, en suivant un peu l'esprit de ceux des ECQ. La positivité va pourtant changer les choses, notamment lorsque l'on prendra le bipolaire positif d'un ensemble d'opérateurs.

11.3.1 Additifs

Définition 11.8 :

Si A et B sont des ECQ⁺, on pose $A \oplus^+ B$, de trame $|A| \oplus |B|$:

$$A \oplus^+ B := \sim^+ \sim^+ \{ \lambda x \oplus \mu y \mid \lambda, \mu \geq 0, \lambda + \mu \leq 1, x \in A, y \in B \}$$

¹³On note $A \rightarrow^+ B$ pour $A \rightarrow B$ restreint aux superpositifs.

Plus intuitivement, $A \oplus^+ B$ correspond à $A \oplus B$ auquel on aurait ajouté des éléments hors-diagonale pour obtenir tous les positifs dont la version réduite est dans $A \oplus B$.

On définit dualement : $A \&^+ B := \sim^+ ((\sim^+ A) \oplus^+ (\sim^+ B))$. On peut également définir le $\&^+$ directement.

Proposition 11.9 :

|| Si A et B sont des ECQ^+ , on a $A \&^+ B = \{h \in \mathcal{H}^+(|A| \oplus |B|) \mid \pi_{|A|} h \pi_{|A|} \in A \text{ et } \pi_{|B|} h \pi_{|B|} \in B\}$

Preuve : posons $X := \{h \in \mathcal{H}^+(|A| \oplus |B|) \mid \pi_{|A|} h \pi_{|A|} \in A \text{ et } \pi_{|B|} h \pi_{|B|} \in B\}$ et $Y := \{\lambda x \oplus \mu y \mid x \in \mathcal{H}^+(|A|) \ y \in \mathcal{H}^+(|B|) \ \lambda, \mu \geq 0, \lambda + \mu \leq 1 \ x \in \sim^+ A \ y \in \sim^+ B\}$.

Soit $h \in \mathcal{H}^+(|A| \oplus |B|)$, on pose $h_A := \pi_{|A|} h \pi_{|A|}$ et $h_B := \pi_{|B|} h \pi_{|B|}$.

Si $h \in X$, soit $g \in Y$. On a $Tr({}^t gh) = Tr(\lambda {}^t x h_A) + Tr(\mu {}^t y h_B) < 1$ car $x \in \sim^+ A$, $y \in \sim^+ B$ et $\lambda + \mu \leq 1$. Donc $h \in \sim^+ Y$.

C'est à dire $X \subseteq \sim^+ Y$

Réciproquement, si h n'est pas dans X , alors on a $h_A \notin A$ ou $h_B \notin B$. Supposons que $h_A \notin A$, le problème étant parfaitement symétrique.

On a alors, A étant un ECQ^+ , $w \in \sim^+ A$ tel que $Tr(wh_A) > 1$. Mais alors, $w' := w \oplus 0_{|B|}$ appartenant à Y et $Tr(w'h) = Tr(wh_A) > 1$, on a $h \notin \sim^+ Y$

Donc $X = \sim^+ Y$. Comme $\sim^+ A \oplus \sim^+ B = \sim^+ \sim^+ Y$, on a

$X = \sim^+ Y = \sim^+ \sim^+ \sim^+ Y = \sim^+ (\sim^+ A \oplus^+ \sim^+ B)$. ★

11.3.2 Multiplicatifs

Pour définir les connecteurs multiplicatifs, on va suivre les idées de la discussion en 10.1. On commence donc par définir l'implication linéaire :

Définition 11.10 :

Si A et B sont des ECQ^+ , on définit $A \rightarrow^+ B$ par

$$A \rightarrow^+ B := \{\chi_F \mid F \in a \rightarrow^+ B\}$$

Ceci nous permet de dériver les connecteurs \otimes^+ et \wp^+ comme en 7.3.2.

Ici aussi, on peut donner une définition alternative d'un des connecteurs :

Proposition 11.11 :

|| Si A et B sont des ECQ^+ , on a $A \otimes^+ B = \sim^+ \sim^+ \{a \otimes b \mid a \in A, b \in B\}$

|| Ceci prouve également que $A \otimes^+ B$ et donc $A \rightarrow^+ B$ et $A \wp^+ B$ sont des ECQ^+ .

Preuve : on note X l'ensemble $\{a \otimes b \mid a \in A, b \in B\}$.

Si $x \otimes y \in X$, et $\chi_F \in A \rightarrow^+ (\sim^+ B)$, on a $Tr(\chi_F \cdot {}^t(x \otimes y)) = Tr(\chi_F \cdot {}^t x \otimes {}^t y) = Tr(F(x) \cdot {}^t y)$.

Comme $F \in A \rightarrow^+ (\sim^+ B)$, on a $\chi_F \downarrow^+ x \otimes y$.

Ceci valant pour tout $F \in A \rightarrow^+ (\sim^+ B) = \sim^+ (A \otimes^+ B)$, on a $x \otimes y \in A \otimes^+ B$.

On a donc $X \subseteq A \otimes^+ B$ et $\sim^+ \sim^+ X \subseteq A \otimes^+ B$.

Réciproquement, soit $\chi_F \in A \rightarrow^+ (\sim^+ B)$. Soit $x \otimes y \in X$. On a par le même calcul $\chi_F \downarrow^+ x \otimes y$ et donc $\chi_F \in \sim^+ X$. Par décroissance de \sim^+ pour l'inclusion, on a bien $A \otimes^+ B \subseteq \sim^+ \sim^+ X$. ★

11.3.3 Distributivité

On a toujours l'isomorphisme de la section 7.3.3.

Proposition 11.12 : distributivité

\otimes^+ distribue sur \oplus^+ , :
 pour tous A, B, C $A \otimes^+ (B \oplus^+ C) \simeq (A \otimes^+ B) \oplus^+ (A \otimes^+ C)$
 Dualement, \wp^+ distribue sur $\&^+$.

Preuve : on fait la même démonstration que pour 7.3.3. La seule chose à vérifier est que l'isomorphisme est bien superpositif, ce qui est une conséquence du théorème 9. ★

11.4 Booléens et connecteurs

On va maintenant revenir sur l'exemple des booléens quantiques, pour voir ce qui change avec la restriction aux positifs.

Les définitions ne changent pas car les booléens et anti-booléens quantiques sont des ECQ^+ :

Proposition 11.13 :

Soit H un espace de hilbert de dimension finie :
 1. $P_{H^*} = \{ {}^t h \mid h \in P_H \}$ et $N_{H^*} = \{ {}^t h \mid h \in N_H \}$
 2. $\sim^+ P_H = N_{H^*}$
 3. P_H et N_H sont des ECQ^+

Preuve :
 On utilise le corollaire 10.7 : la transposée préserve la positivité, la trace et la norme des opérateurs.
 On en déduit que ${}^t P_H \subseteq P_{H^*}$ et ${}^t N_H \subseteq N_{H^*}$ mais comme la transposée est involutive et que $(H^*)^* = H$, on a

$$P_{H^*} = {}^t {}^t P_{H^*} \subseteq {}^t P_{(H^*)^*} = {}^t P_H$$

d'où $P_{H^*} = {}^t P_H$ et $N_{H^*} = {}^t N_H$.

Comme la transposée conserve la trace et la norme triple, pour les mêmes raisons que pour les espaces cohérents quantiques, $N_{H^*} \subseteq \sim^+ P_H$ et $P_{H^*} \subseteq \sim^+ N_H$.

Montrons que $\sim^+ P_H \subseteq N_{H^*}$.

Soit $n \in \sim^+ P_H$ et ${}^t n$ sa transposée. Soit $|\psi\rangle$ le vecteur de H tel que $\langle \psi | {}^t n | \psi \rangle = ||| {}^t n ||| = ||| n |||$. L'opérateur $|\psi\rangle\langle \psi |$ est dans P_H , donc

$$||| n ||| = Tr({}^t n |\psi\rangle\langle \psi |) \leq 1$$

et n appartient bien à N_{H^*} . D'où $N_{H^*} = \sim^+ P_H$. L'ensemble N_H est un espace cohérent quantique.

Montrons que $\sim^+ N_{H^*} \subseteq P_H$.

Soit $\rho \in \sim N_{H^*}$. L'identité de H^* appartient à N_{H^*} donc

$$Tr(\rho) = Tr(\rho Id_H) = Tr(\rho {}^t Id_{H^*}) \leq 1$$

donc ρ appartient à P_H . D'où $P_H = \sim^+ N_{H^*}$. L'ensemble P_H est un espace cohérent quantique. ★

On va voir que l'on perd un peu sur le \otimes^+ de deux booléens quantiques qui, s'il est toujours l'espace cohérent engendré par les séparables, n'est plus simplement son enveloppe convexe. En revanche,

le connecteur \mathfrak{F}^+ se comporte beaucoup mieux et permet de former l'espace de **tous** les états sur le produit tensoriel des trames, y compris les états intriqués. Comme on se restreint ici aux positifs, on obtient exactement ces états et rien "en trop" comme c'était le cas auparavant.

Théorème 11 : états séparables

Soient H_1 et H_2 deux espaces de Hilbert. On note encore Sep l'ensemble des matrices de densité représentant un état séparable de $H_1 \otimes H_2$, i.e. Sep est l'enveloppe convexe de l'ensemble $X := \{\rho_1 \otimes \rho_2 \mid \forall i \rho_i \geq 0, Tr(\rho_i) = 1\}$. On a alors :

$$P_{H_1} \otimes^+ P_{H_2} = \sim^+ \sim^+ Sep$$

Preuve :

Soit Y l'ensemble engendrant $P_{H_1} \otimes^+ P_{H_2}$ c'est-à-dire, $Y = \{\rho_1 \otimes \rho_2 \mid \rho_1 \in P_{H_1} \text{ et } \rho_2 \in P_{H_2}\}$.

Montrons que Sep est inclus dans $P_{H_1} \otimes^+ P_{H_2}$.

En effet, pour tout x , l'opération $y \mapsto Tr(y^t x)$ étant linéaire et le segment $[0, 1]$ étant convexe, les espaces cohérents positifs, dont $P_{H_1} \otimes^+ P_{H_2}$, restent des convexes (fermés de surcroît). Or, X est inclus dans Y donc son enveloppe convexe Sep est inclus dans l'enveloppe convexe de Y elle-même contenue dans $\sim^+ \sim^+ Y$ puisque cet ensemble est un convexe contenant Y .

On en déduit que $\sim^+ \sim^+ Sep \subseteq \sim^+ \sim^+ Y = P_{H_1} \otimes^+ P_{H_2}$.

Réciproquement, Y est inclus dans $[0, 1]Sep$, qui est l'enveloppe convexe de $\{0\} \cup Sep$. Or, 0 appartient à tout espace cohérent positif donc $\{0\} \cup Sep$ est inclus dans $\sim^+ \sim^+ Sep$ et donc son enveloppe convexe $[0, 1]Sep$ aussi. On a donc $Y \subseteq \sim^+ \sim^+ Sep$.

On en déduit que $P_{H_1} \otimes^+ P_{H_2} = \sim^+ \sim^+ Y \subseteq \sim^+ \sim^+ Sep$.

Finalement, on a bien $P_{H_1} \otimes^+ P_{H_2} = \sim^+ \sim^+ Sep$. ★

Théorème 12 : \mathfrak{F}^+ et intrication

Soient H_1 et H_2 des espaces de Hilbert de dimensions finies. On a :

$$P_{H_1} \mathfrak{F}^+ P_{H_2} = P_{H_1 \otimes H_2}$$

Preuve : Par définition, l'ECQ⁺, $P_{H_1} \mathfrak{F}^+ P_{H_2}$ est le polaire de l'ensemble :

$$N := \{n_1 \otimes n_2 \mid n_1 \in N_{H_1}^*, n_2 \in N_{H_2}^*\}.$$

Soit $\rho \in P_{H_1} \mathfrak{F}^+ P_{H_2}$. Par définition des ECQ⁺, ρ est positif. De plus, comme les identités de H_1^* et H_2^* appartiennent respectivement à $N_{H_1}^*$ et $N_{H_2}^*$, leur produit tensoriel, à savoir l'identité de $H_1^* \otimes H_2^*$, appartient à N , car sa transposée n'est autre que l'identité Id de $H_1 \otimes H_2$.

On en déduit que la trace de ρ est inférieure ou égale à 1. En effet,

$$Tr(\rho) = Tr(\rho Id) \in [0, 1]$$

par polarité.

On a bien $\rho \in P_{H_1 \otimes H_2}$.

Réciproquement, si $\rho \in P_{H_1 \otimes H_2}$, alors pour tout $n_1 \in N_{H_1}^*$ et $n_2 \in N_{H_2}^*$, on a :

$$Tr(\rho^t(n_1 \otimes n_2)) \leq Tr(\rho) |||n_1 \otimes n_2||| = Tr(\rho) |||n_1||| |||n_2|||$$

Or, $Tr(\rho) \leq 1$, $|||n_1||| \leq 1$ et $|||n_2||| \leq 1$ donc

$$Tr(\rho^t(n_1 \otimes n_2)) \in [0, 1]$$

Autrement dit, ρ est dans le polaire de N , c'est-à-dire dans $P_{H_1} \wp^+ P_{H_2}$.

★

11.5 Positivité et dimension infinie

Depuis le début de ce mémoire, on n'a manipulé que des espaces de dimension finie. La raison étant que le point de départ de la construction, la trace, n'est pas définie sur tout $\mathcal{H}(H_1)$ pour H_1 de dimension infinie.

Pourtant, la dimension infinie semble être le bon endroit pour interpréter l'exponentielle. On pense en particulier à l'espace de Fock symétrique qui présente une bonne analogie avec les multi-ensembles qui fournissent un modèle de l'exponentielle dans le cas discret.

Dans [8], plusieurs solutions sont envisagées pour contourner le problème de non-définition de la trace :

- Se restreindre à l'idéal bilatère des opérateurs à trace. Cette solution ne conserve aucun opérateur inversible, et donc ne conserve pas le "twist" dans le cas de $X \rightarrow X$. On n'aurait donc pas θ_{Id} dans $X \rightarrow X$.
- Se placer dans un « facteur de type II_1 » où la trace est finie. Cette solution impose de nombreux changements au modèle pour aller vers la *géométrie de l'interaction*, qui est « une tout autre histoire ».
- Même si la trace n'est pas définie sur tout $\mathcal{H}(H_1)$, elle a un sens comme élément de $[0, +\infty]$ pour les opérateurs *positifs* (on parle alors de trace semi-finie). Malheureusement, on bute encore sur le problème du "twist" qui n'est pas positif.

Or, on vient justement de voir qu'en changeant d'isomorphisme entre $X \rightarrow Y$ et $\sim X \wp Y$, on pouvait se restreindre aux opérateurs positifs sans perdre l'image de l'identité dans $X \rightarrow X$, ce qui efface potentiellement l'obstacle à la troisième solution : utiliser une trace semi-finie sur les opérateurs bornés positifs d'un espace de Hilbert de dimension infinie.

Bien que cela promette un certain nombre de complications techniques, on pourrait essayer de voir jusqu'où cette construction peut être poussée. En particulier, étudier plus en détails la possibilité d'interpréter l'exponentielle dans des espaces aux symétries différentes (bosoniques et fermioniques) pourrait être très intéressant.

11.6 Un autre exemple : l'électron et le positron

La première prévision théorique de l'existence d'antimatière est dûe à Dirac et son équation, admettant des solutions sans interprétation physique à cette époque, qu'il a interprété comme une nouvelle particule, le positron, antiparticule de l'électron.

Quand une particule est confrontée à son antiparticule, celles-ci s'annihilent. Or, en logique linéaire, on assiste au même phénomène lorsqu'on confronte A et $\sim^+ A$. On va donc pour cela interpréter un électron comme un espace cohérent A et voir que le polaire de A interprète de façon analogue les positrons.

11.6.1 Espaces cohérents positifs et projections

Soit H un espace de Hilbert et G un sous-espace de Hilbert de H . On note G^\perp son orthogonal et P la projection orthogonale de H sur G .

Définition 11.14 :

On note A_G l'ensemble des opérateurs positifs sur H nuls sur G^\perp . Autrement dit,

$$A_G = \{ p \geq 0 \mid PpP = p \}.$$

On a la propriété suivante :

Proposition 11.15 :

L'ensemble A_G est un espace cohérent positif et admet pour polaire :

$$\sim^+ A_G = {}^t A_{G^\perp}.$$

Preuve : Soit $p \in A_G$ et $p^\perp \in A_{G^\perp}$. Comme la projection orthogonale sur G^\perp est $1 - P$, on a :

$$\text{Tr}(pp^\perp) = \text{Tr}(PpP(1 - P)p^\perp(1 - P))$$

Or, $P(1 - P) = P - P^2 = P - P = 0$, donc

$$\text{Tr}(pp^\perp) = \text{Tr}(0) = 0.$$

On en déduit que ${}^t A_{G^\perp}$ est inclus dans le polaire de A_G .

Montrons l'inclusion réciproque. Soit $\tilde{n} \in \sim^+ A_G$ et $n = {}^t \tilde{n}$ sa transposée. Pour tout vecteur $|\psi\rangle$ de G , et r réel positif, l'opérateur $r|\psi\rangle\langle\psi|$ appartient à A_G donc :

$$r\langle\psi|n|\psi\rangle = \text{Tr}(r|\psi\rangle\langle\psi|n) \in [0, 1]$$

$$\langle\psi|n|\psi\rangle = 0.$$

Mais comme PnP est un opérateur positif, on en déduit que $PnP = 0$.

Autrement dit, n se met sous la forme

$$n = Pn(1 - P) + (1 - P)nP + (1 - P)n(1 - P)$$

Soit $|u\rangle \in G$ et $|v\rangle \in G^\perp$, on a, comme n est positif :

$$\langle u + v|n|u + v\rangle = 2\text{Re}(\langle u|n|v\rangle) + \langle v|n|v\rangle \geq 0$$

En remplaçant $|v\rangle$ par $r|v\rangle$ où r est un réel positif, on obtient $2r\text{Re}(\langle u|n|v\rangle) + r^2\langle v|n|v\rangle \geq 0$, en divisant par r , $2\text{Re}(\langle u|n|v\rangle) + r\langle v|n|v\rangle \geq 0$ puis en faisant tendre r vers 0, on a :

$$2\text{Re}(\langle u|n|v\rangle) \geq 0$$

Enfin, en changeant $|u\rangle$ en $-|u\rangle$, on obtient $\text{Re}(\langle u|n|v\rangle) = 0$ et en $i|u\rangle$, on a :

$$\langle u|n|v\rangle = 0$$

pour tout $|u\rangle \in G$ et $|v\rangle \in G^\perp$, autrement dit $Pn(1 - P) = 0$, et donc $(1 - P)nP = (Pn(1 - P))^* = 0$, n se met sous la forme :

$$n = (1 - P)n(1 - P).$$

L'opérateur n appartient donc bien à A_{G^\perp} .

D'où ${}^t A_{G^\perp} = \sim^+ A_G$.

On en déduit que $\sim^+ \sim^+ A_G = \sim^+ ({}^t A_{G^\perp}) = {}^t \sim^+ A_{G^\perp} = {}^{tt} A_{(G^\perp)^\perp}$. Or la transposée est involutive et $(G^\perp)^\perp = G$ donc $\sim^+ \sim^+ A_G = A_G$. L'ensemble A_G est un espace cohérent positif. ★

Remarque : on ne retrouve pas ce résultat avec les ECQ classiques. D'une part, A_G ne vérifie pas les conditions imposées par le théorème du Bipolaire, et donc n'est pas un espace cohérent quantique. D'autre part, son polaire (en tant qu'ensemble) ne contient pas nécessairement que des opérateurs

positifs, comme on l'impose pour les espaces cohérents positifs, donc ses éléments admettent des coefficients par bloc hors diagonaux.

11.6.2 Equation de Dirac

On s'intéresse à l'évolution libre d'une particule. L'équation de Dirac décrit l'évolution d'un électron ou d'un positron en l'absence de champ ou de toute autre particule.

Dirac part de la relation énergie-moment relativiste :

$$E^2 = c^2 p^2 + m^2 c^4$$

où E est l'énergie, c la vitesse de la lumière, m la masse de la particule, et p son impulsion.

En mécanique quantique, on fait la substitution :

$$\begin{cases} E \leftarrow i\hbar\partial_t, \\ p \leftarrow -i\hbar\nabla \end{cases}$$

La relation énergie-impulsion correspond alors à l'équation de Klein-Gordon :

$$-\hbar^2\partial_t^2\psi = (-\hbar^2c^2\Delta + m^2c^4)\psi.$$

Afin de réduire cette équation d'onde en deux équations d'ordre 1 par rapport au temps, Dirac propose d'utiliser des matrices. En d'autres termes, il cherche des opérateurs (α_i) pour $i = 1, 2, 3$ et β tels que l'équation :

$$i\hbar\partial_t\psi = \left(\sum_i \alpha_i p_i + \beta mc^2\right)\psi$$

élevée au carré redonne l'équation de Klein-Gordon. En réalité, Dirac cherchait des nombres α_i et β , cependant les relations que ces objets doivent vérifier :

$$\begin{cases} \alpha_i\alpha_j + \alpha_j\alpha_k = 2\delta_{i,k} & i, k = 1, 2, 3 \\ \alpha_i\beta + \beta\alpha_i = 0 & i = 1, 2, 3 \\ \beta^2 = 1 \end{cases}$$

en font des opérateurs de dimension au moins 4×4 .

Une solution pour cet ensemble d'égalité est :

$$\beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

et

$$\alpha_i = \begin{pmatrix} 0 & \sigma_i \\ \sigma_i & 0 \end{pmatrix}$$

où les σ_i sont les matrices (2×2) de Pauli :

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On obtient alors l'équation de Dirac :

$$i\hbar\partial_t\psi = H_0\psi$$

où H_0 est le Hamiltonien :

$$H_0 = -i\hbar c \vec{\alpha} \vec{\nabla} + \beta mc^2 = \begin{pmatrix} mc^2 Id & -i\hbar \vec{\sigma} \vec{\nabla} \\ -i\hbar \vec{\sigma} \vec{\nabla} & -mc^2 Id \end{pmatrix}.$$

Ce Hamiltonien est un opérateur auto-adjoint de l'espace de Hilbert $H^1(\mathbb{R}^3)^4$. Son spectre est $]-\infty, -mc^2] \cup [mc^2, \infty[$. De plus, tout vecteur propre d'énergie (de valeur propre) positive E de H_0 correspond à un vecteur propre d'énergie $-E$ de H_0 . Les solutions d'énergie positive s'interprètent usuellement comme les états possibles de l'électron. En revanche, les états d'énergie négative (et surtout dont l'énergie tend vers $-\infty$) posent problème.

La solution que propose Dirac, en analogie avec le comportement des particules en présence d'un champ, est d'interpréter ces solutions d'énergie $-E$ comme des particules de même masse que l'électron m , d'énergie E mais de charge opposée $+e$: c'est la première prédiction théorique de l'existence des positrons.

11.6.3 Lien avec les espaces cohérents positifs

Soit E_1, \dots, E_n des valeurs propres de H_0 associés aux vecteurs propres $|\psi_1^+\rangle, \dots, |\psi_n^+\rangle$. Le Hamiltonien H_0 admet des vecteurs propres correspondante, $|\psi_1^-\rangle, \dots, |\psi_n^-\rangle$ de valeur propres $-E_1, \dots, -E_n$. En d'autres termes, pour chaque électron d'énergie E_i , on considère son antiparticule de même énergie.

En posant $H = Vect(|\psi_1^+\rangle, \dots, |\psi_n^+\rangle, |\psi_1^-\rangle, \dots, |\psi_n^-\rangle)$, $H^+ = Vect(|\psi_1^+\rangle, \dots, |\psi_n^+\rangle)$ et $H^- = Vect(|\psi_1^-\rangle, \dots, |\psi_n^-\rangle)$, on obtient la somme orthogonale :

$$H = H^+ \oplus H^-.$$

D'après ce qu'on a vu précédemment les espaces A_{H^+} et A_{H^-} sont des espaces cohérents positifs et

$$\sim^+ A_{H^+} = {}^t A_{H^-} = A_{(H^-)^*}$$

le polaire de l'espace des électrons d'énergies E_1, \dots, E_n est donc canoniquement isomorphe à l'espace des positrons de mêmes énergies.

Confronter les formules A et $\sim^+ A$ à travers la règle de coupure "annihile" les formules A et $\sim^+ A$. Remarquons néanmoins que ces formules interagissent dans un environnement. En effet, la règle de coupure s'écrit

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, \sim^+ A}{\vdash \Gamma, \Delta} (Cut)$$

Autrement dit, les formules A et $\sim^+ A$ interagissent via l'environnement réunissant les multiensembles de formules Γ et Δ . A priori, ces multiensembles peuvent être vides, mais on peut montrer qu'au moins l'un des deux ne l'est pas, puisque le séquent $\vdash \emptyset$ voire $\vdash \perp$ (\perp étant l'élément neutre de \mathfrak{F}) n'a pas de sens.

On a donc besoin d'un élément extérieur pour faire interagir deux formules polaires.

Dans un certain sens, cela rappelle le fait qu'en confrontant un électron à un positron en les faisant interagir par le biais d'un photon, les deux particules s'annihilent également. Mais une fois de plus, l'électron et le positron sont plongés dans leur environnement. Seuls, en parfaite solutions de l'équation de Dirac, ils ne peuvent pas être confrontés l'un à l'autre.

Finalement, on peut imaginer que l'électron et le positron pris séparément sont comme les formules A_{H^+} et $A_{(H^-)^*}$ pris dans des séquents différents. À partir du moment où on les réunit grâce à une règle de coupure, leur environnement entre en jeu et leur permet de se détruire mutuellement.

12 Interprétation des preuves

On va maintenant décrire la façon dont les ECQ¹⁴ permettent d'interpréter les preuves de logique linéaire. Pour le cas des espaces cohérents classique, voir par exemple [6], chapitre 9.

L'idée est que l'on va associer à toute démonstration d'un séquent $\Gamma \vdash B$ un élément de $\llbracket \Gamma \rrbracket \rightarrow \llbracket B \rrbracket$ (en fait une application de $\llbracket \Gamma \rrbracket \rightarrow \llbracket B \rrbracket$, à travers l'isomorphisme $[\cdot]$). On définit donc l'interprétation récursivement, règle par règle.

On arrive ainsi à interpréter le fragment parfait de la logique linéaire, généralement appelé MALL (pour **m**ultiplicative **a**dditive **l**inear **l**ogic).

Interprétation des formules :

On considère que les formules que l'on manipule sont formées à partir de formules atomiques qu'on notera X_1, X_2, \dots , des connecteurs de la logique linéaire ($\oplus, \otimes, \wp, \&$) et de la négation linéaire.

On peut alors définir l'interprétation $\llbracket \cdot \rrbracket$:

- Les formules atomiques sont interprétés par les booléens de dimension 2, $\llbracket X_i \rrbracket := P_{\mathbb{C} \otimes \mathbb{C}}$
- Les formules composées sont interprétées de façon transparente :
 - $\llbracket \sim A \rrbracket := \sim \llbracket A \rrbracket$
 - $\llbracket A \otimes B \rrbracket := \llbracket A \rrbracket \otimes \llbracket B \rrbracket$
 - $\llbracket A \oplus B \rrbracket := \llbracket A \rrbracket \oplus \llbracket B \rrbracket$
 - $\llbracket A \wp B \rrbracket := \llbracket A \rrbracket \wp \llbracket B \rrbracket$
 - $\llbracket A \& B \rrbracket := \llbracket A \rrbracket \& \llbracket B \rrbracket$
- Une suite de formules $\Gamma = A_1, A_2, \dots, A_n$ gauche du symbole \vdash sera interprétée par : $\llbracket A_1 \rrbracket \otimes \llbracket A_2 \rrbracket \otimes \dots \otimes \llbracket A_n \rrbracket$. À droite du symbole \vdash , on l'interprètera par $\llbracket A_1 \rrbracket \wp \llbracket A_2 \rrbracket \wp \dots \wp \llbracket A_n \rrbracket$.

Cependant, pour une meilleure lisibilité on ne notera pas les $\llbracket \cdot \rrbracket$ s'il n'y a pas de risque de confusion entre la formule et l'espace cohérent associé.

Interprétation des preuves

On ne regarde que certains cas, en particulier ceux qui nous serviront dans la sous-section suivante.

Notation :

$$f : \frac{\vdots}{\Gamma \vdash A}$$

signifie que l'application f interprète la preuve de $\Gamma \vdash A$.

Axiome :

$$Id_{\mathcal{H}(|A|)} : \frac{}{A \vdash A}$$

L'axiome s'interprète par une identité.

Tenseur :

$$f \otimes g : \frac{f : \frac{\vdots}{\Gamma \vdash A} \quad g : \frac{\vdots}{\Delta \vdash B}}{\Gamma \vdash A \otimes B}$$

La règle du \otimes s'interprète en formant le produit tensoriel des applications linéaires interprétant les deux preuves que l'on combine.

¹⁴On donne l'interprétation pour les ECQ, mais cela fonctionne également dans le cas des ECQ⁺.

Avec :

$$f \oplus g : \frac{\frac{\vdots}{\Gamma \vdash A} \quad \frac{\vdots}{\Gamma \vdash B}}{\Gamma \vdash A \& B}$$

La règle du & correspond à une somme directe des interprétations des deux preuves concernées.

Plus droit :

$$i_A \circ f : \frac{\frac{\vdots}{\Gamma \vdash A}}{\Gamma \vdash A \oplus B}$$

(où i_A est l'injection des opérateurs de la trame de $[[\Gamma, A]]$ dans ceux de trame de $[[\Gamma, A \& B]]$)

Le plus gauche correspond à composer avec une injection qui plonge l'espace d'arrivée du morphisme de départ dans un espace plus grand.

En utilisant l'isomorphisme $[\cdot]$, on peut en déduire une forme équivalente qui nous servira dans la suite :

$$f \circ \pi_A : \frac{\frac{\vdots}{\Gamma, A \vdash C}}{\Gamma, A \& B \vdash C}$$

(où π_A est la projection des opérateurs de la trame de $[[\Gamma, A \& B]]$ sur ceux de la trame de $[[F, A]]$)

Nous n'allons pas étudier en détail les propriétés de cette interprétation. Regardons simplement un des points sur lesquels les ECQ se démarquent des modèles plus classiques de la logique linéaire, la η -conversion.

12.1 η en logique

La logique informatique s'intéresse avant tout à la *dynamique* des preuves, et les questions sur les façons de réécrire des preuves forment donc le sujet central de ce domaine.

On a déjà parlé d'une première façon de réduire les preuves : l'élimination des coupures (qu'on appelle souvent β -réduction). Il existe autre chose que l'on peut chercher à éliminer : les *identités*. Plus précisément, on peut chercher à voir la différence entre une identité *globale*, comme dans la preuve :

$$\frac{}{A \& B \vdash A \& B} \text{Axiome}$$

et un "recollement" de deux identités, comme dans la preuve :

$$\frac{\frac{\frac{}{A \vdash A} \text{(Axiome)}}{A \& B \vdash A} \text{(Plus droit)} \quad \frac{\frac{\frac{}{B \vdash B} \text{(Axiome)}}{A \& B \vdash B} \text{(Plus gauche)}}{A \& B \vdash A \& B} \text{(Avec)}}{A \& B \vdash A \& B}$$

Une autre façon d'aborder le sujet est de dire que l'on se pose la question : « peut-on réduire une formule à la combinaison de ses sous-formules ? »

La plupart des modèles classiques ne font pas la différence entre les deux, tout simplement parce que si les objets que l'on manipule sont des ensembles :

$$(Id_A, Id_B) : A \times B \rightarrow A \times B \text{ est exactement la même chose que } Id_{A \times B}$$

On finit donc par dire que la deuxième preuve (qu'on appelle forme η -expansée de la première) est "plus réduite" que la première, mais de façon relativement arbitraire.

12.2 η dans les ECQ

Les ECQ vont faire profiter de leur point de vue quantique, dans lequel justement un système ne peut se réduire à ses sous-systèmes quand il y a intrication.

En fait, on peut reprendre l'exemple ci-dessus et voir que l'interprétation des deux preuves est différente dans les ECQ.

Évidemment, on obtient toujours la vraie identité dans le premier cas

$$Id_{\mathcal{H}(|A| \oplus |B|)} : \frac{}{A \& B \vdash A \& B}$$

Mais la deuxième preuve donne par contre :

$$(Id_{\mathcal{H}(|A|)} \circ \pi_A) \oplus (Id_{\mathcal{H}(|B|)} \circ \pi_B) : \frac{\frac{}{A \vdash A} \quad \frac{}{B \vdash B}}{A \& B \vdash A} \quad \frac{}{A \& B \vdash B}}{A \& B \vdash A \& B}$$

Si on représente les opérateurs par des matrices par blocs (correspondant à la décomposition $|A| \oplus |B|$), on voit que l'action du morphisme interprétant la deuxième preuve est :

$$\begin{pmatrix} U & W \\ W^\dagger & V \end{pmatrix} \longrightarrow \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix}$$

c'est à dire une identité pour les opérateurs déjà réduits par rapport à la décomposition en $|A| \oplus |B|$. Cela revient en fait à effectuer une mesure "sans lecture" de l'état du système. Cela se comprend mieux sur un exemple. Supposons que l'on interprète A et B par l'élément neutre 1. Notons ϕ l'application qui interprète la preuve. On a :

$$\phi \left[\frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

On voit que ϕ réduit l'état superposé $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, représenté par la matrice $\frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, en un simple mélange statistique correspondant aux probabilités d'obtenir $|0\rangle$ ou $|1\rangle$ en effectuant une mesure.

Dans [6], J.-Y. Girard appelle cela l'identité « du gendarme », qui demande ses papiers à l'opérateur, puis le laisse passer. Mais en mécanique quantique, demander les papiers d'un opérateur, c'est faire une mesure (sans lecture dans notre cas) qui modifie l'état du système.

Le modèle n'identifie plus une preuve et sa version η -réduite, ce qui plaide plutôt contre la η -équivalence, du moins quand on cherche à adopter un point de vue quantique.

13 Conclusion

Nous nous sommes surtout attachés dans ce mémoire aux aspects techniques du modèle des ECQ, et sa correspondance avec les notions de mécanique quantique dont il s'inspire. Le point principal étant la discussion sur la positivité des opérateurs. On peut en résumer les étapes importantes :

On a vu que le \wp de deux ECQ constitués uniquement d'opérateurs positifs peut contenir des opérateurs qui ne sont pas positifs. Ceci est lié au fait que les transformations envisagées pour interpréter les preuves ne sont pas toutes superpositives.

De plus, quelles que soient les dimensions de H_1 et H_2 , $P_{H_1} \wp P_{H_2}$ contient un opérateur admettant $-\frac{1}{2}$ comme valeur propre. Ceci enlève tout espoir que la dimension infinie "tue" les valeurs propres négatives des opérateurs que l'on considère. Or, c'est justement la possibilité d'avoir des valeurs propres négatives qui empêche de donner une notion de trace en dimension infinie.

On a ensuite constaté que l'on pouvait avoir un modèle qui fonctionne en se restreignant aux opérateurs positifs, en changeant d'isomorphisme entre $A \rightarrow B$ et $\sim A \wp B$. Cette approche semble plus satisfaisante du point de vue physique (l'état des systèmes physiques utilise des matrices densité, positives) et permet d'envisager une extension en dimension infinie. La trace serait alors remplacée par la notion de trace *semi-finie*, définie uniquement sur les opérateurs positifs, et à valeurs dans $[0, +\infty]$.

L'intérêt d'étendre la construction à des espaces de dimension infinie est que cela pourrait permettre d'interpréter la modalité exponentielle, ou au moins quelque-chose d'approchant, dans les ECQ. En effet, l'espace de Fock symétrique (le cas anti-symétrique semble moins adapté mais pourrait être étudié malgré tout) présente des propriétés géométriques qui font penser à celles de l'exponentielle. En particulier on a un isomorphisme $\mathbb{S}(U \oplus V) \simeq \mathbb{S}(H_1) \otimes \mathbb{S}(H_2)$ qui fait évidemment penser à un isomorphisme fondamental en logique linéaire : $!(A \& B) \simeq !A \otimes !B$

Un fois maîtrisés ces questions techniques, on pourra chercher à voir ce qu'apporte le modèle des ECQ (ou des ECQ⁺) à la compréhension de la logique linéaire. On a vu en 12, un début de réflexion, sur le thème de l' η -expansion qui acquiert un vrai statut dans le modèle des ECQ.

Mais il y a d'autres pistes à étudier :

- la question des connecteurs additifs reste traitée assez partiellement, car on n'a pas défini de connecteur correspondant au "plus quantique", *i.e.*, tel que $P_{H_1} \oplus_{\text{Qu.}} P_{H_2} = P_{H_1 \oplus H_2}$
- en physique, on construit les espaces de Fock à l'aide de leurs opérateurs de création et d'annihilation. Ceux-ci correspondent respectivement à faire entrer une particule dans le système et à détruire une particule du système. Si l'on arrivait à interpréter l'exponentielle dans les espaces de Fock, cela justifierait des règles logiques de la forme

$$\frac{X, !X, \Gamma \vdash \Delta}{!X, \Gamma \vdash \Delta} \text{ (Anihilation)} \qquad \frac{!X, \Gamma \vdash \Delta}{X, !X, \Gamma \vdash \Delta} \text{ (Création)}$$

qui ne sont pas sans rappeler la *logique linéaire différentielle* de Thomas Ehrhard.

Ainsi, en mettant à jour des structures n'apparaissant pas dans les modèles ensemblistes, les ECQ pourraient contribuer à une relecture quantique de la logique linéaire.

A Annexe

A.1 Les règles de la logique linéaire

Pour les non-logiciens : comment lire un séquent ?

Les séquents sont une notation inventée par Gentzen utilisée pour rendre les preuves plus maniables et qui a permis de mieux comprendre leur géométrie.

L'idée de départ est simple : écrire

$$A_1, A_2, \dots, A_n \vdash B_1, B_2, \dots, B_m$$

à la place de

$$A_1 \text{ 'et' } A_2 \text{ 'et' } \dots A_n \Rightarrow B_1 \text{ 'ou' } B_2 \text{ 'ou' } \dots B_m$$

Une démonstration en calcul des séquents est un enchaînement d'étapes de la forme :

$$\frac{\Gamma_1 \vdash \Delta_1 \dots \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

(où $\Gamma_i, \Delta_i \dots$ représentent des multi-ensembles¹⁵ de formules.)

qui finissent par former ce qu'on appelle un **arbre de preuve**.

En logique linéaire démontrer le séquent $A_1, A_2, \dots, A_n \vdash B_1, B_2, \dots, B_m$ revient à démontrer la formule $A_1 \otimes A_2 \dots \otimes A_n \multimap B_1 \wp B_2 \dots \wp B_m$.

Les règles de la logique linéaire, présentées en forme gauche/droite :

Axiome, implication et négation :

$$\frac{}{A \vdash A} \text{ (Axiome)}$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2, A \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \text{ (Coupure)}$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \sim A \vdash \Delta} \text{ (Négation)}$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \sim A, \Delta} \text{ (Négation)}$$

Multiplicatifs :

$$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} \text{ (Tenseur)}$$

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C} \text{ (Par)}$$

Additifs :

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \& B} \text{ (Avec)}$$

¹⁵C'est-à-dire des ensembles non-ordonnés, mais où un élément peut apparaître plusieurs fois. On peut par exemple parler du multi-ensemble des racines d'un polynôme.

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B} \text{ (Plus gauche)}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash B \oplus A} \text{ (Plus droit)}$$

Exponentielles :

$$\frac{! \Gamma \vdash A}{! \Gamma \vdash ! A} \text{ (Promotion)}$$

($! \Gamma$ signifie que toutes les formules de Γ sont de la forme $! A$)

$$\frac{\Gamma, A \vdash B}{\Gamma, ! A \vdash B} \text{ (Déréliction)}$$

$$\frac{\Gamma \vdash B}{\Gamma, ! A \vdash B} \text{ (Affaiblissement)}$$

$$\frac{\Gamma, ! A, ! A \vdash B}{\Gamma, ! A \vdash B} \text{ (contraction)}$$

A.2 Modélisation des algorithmes quantiques avec controle classique et diminution de la trace

Nous allons expliquer pourquoi on envisage des “états” quantiques de trace inférieure à 1. En réalité, cela est dû à une modélisation des transformations quantiques, en particulier dans un algorithme avec une boucle, à partir d’applications superpositives faisant diminuer la trace.

On va voir que pour modéliser un algorithme qui ne termine pas, on utilise des transformations F telles qu’il existe ρ vérifiant $Tr(F(\rho)) < Tr(\rho)$. Or, ces transformations doivent appartenir à $P_{H_1} \rightarrow P_{H_2}$, où P_{H_1} et P_{H_2} représentent l’ensemble des états de départ et d’arrivée de l’algorithme.

Cependant, il faut faire la distinction entre la transformation F et l’action de l’algorithme. En effet, un algorithme transforme un état normalisé en un autre état normalisé. Tandis que F se contente de représenter cette action, c’est-à-dire qu’elle contient la même information que l’action mais ne fonctionne pas de la même façon. Autrement dit, F appartient à la sémantique de la programmation.

A.2.1 Boucles quantiques

Donnons un exemple : celui de la représentation des boucles.

Supposons que l’on veuille représenter l’algorithme :

```

INPUT :  $\rho$ 
 $b =$  mesure de  $O$ 
Tant que  $f(b)$  faire
 $\rho = U\rho U^*$ 
 $b =$  mesure de  $O$ 
Fin Tant que
Renvoyer  $\rho$ 

```

où O est une observable du système, H_1 une transformation unitaire f est un test classique. On suppose que

$$O = \sum_{i \in I} \lambda_i P_i + \sum_{j \in J} \mu_j P'_j$$

avec pour tout $i \in I$, $f(\lambda_i) = \text{false}$ et pour tout $j \in J$, $f(\mu_j) = \text{true}$.

Décomposons chaque étape en faisant la distinction entre l’action de l’algorithme et sa représentation.

Pour $b =$ mesure de O , on passe de l’état ρ à l’état $\frac{P_i \rho P_i}{Tr(\rho P_i)}$ (resp. $\frac{P'_j \rho P'_j}{Tr(\rho P'_j)}$) où i (resp. j) est l’indice correspondant au résultat de la mesure, *i.e.*, tel que $b = \lambda_i$ (resp. μ_j).

Pour représenter cette mesure dans la sémantique, on considère que le résultat de la mesure est $b = \lambda_i$ (resp. μ_j) avec probabilité $p_i = Tr(\rho P_i)$ (resp. $p'_j = Tr(\rho P'_j)$). On conserve donc ces informations à travers la transformation $M : \rho \mapsto \sum_i P_i \rho P_i + \sum_j P'_j \rho P'_j$. On retrouve $p_i = Tr(M(\rho P_i))$ et $M(\rho)$ est diagonale par blocs sur les espaces propres de O .

En d’autres termes, M transforme ρ en une répartition de probabilité classique sur chaque mesure. Remarquons que M se confond avec l’opération consistant à donner chaque couple $(p_i, \frac{P_i \rho P_i}{p_i})$ et $(p'_j, \frac{P'_j \rho P'_j}{p'_j})$ dans le sens où elle contient exactement la même information.

Une fois qu’on a projeté sur chaque espace propre de l’observable, on peut continuer à agir indépendamment sur l’une ou l’autre des projections.

Par exemple, si l’on veut représenter un test :

```

X = INPUT :  $\rho$ 
 $b =$  mesure de  $O$ 
Si  $f(b)$ 
alors  $\rho = V\rho V^*$ 

```

Sinon $\rho = U\rho U^*$

Fin Si

Renvoyer ρ

L'action de X donne :

$$\left\{ \begin{array}{ll} \frac{UP_i\rho P_i U^*}{Tr(\rho P_i)} & \text{si } b = \lambda_i \quad \text{avec probabilité } Tr(\rho P_i) \\ \frac{VP'_j\rho P'_j U^*}{Tr(\rho P'_j)} & \text{si } b = \mu_j \quad \text{avec probabilité } Tr(\rho P'_j) \end{array} \right.$$

ce qu'on représente par $F(\rho) = \sum_i UP_i\rho P_i U^* + \sum_j VP'_j\rho P'_j U^*$.

Si l'on réapplique le principe de la mesure à $F(\rho)$ (même si $F(\rho)$ n'est pas un état) à travers l'observable $A := \sum_\chi \chi \pi_\chi$ de valeurs propres $\{\chi\}$ et de projecteurs propres les π_χ , on mesure χ avec probabilité :

$$p_\chi = \sum_i p(\chi|b = \lambda_i)p_i + \sum_j p(\chi|b = \mu_j)p'_j$$

où $p(\chi|b = \lambda_i)$ est la probabilité de mesurer χ sachant qu'on a mesuré λ_i auparavant. Autrement dit,

$$p(\chi|b = \lambda_i) = Tr(\pi_\chi \frac{UP_i\rho P_i U^*}{p_i})$$

et donc

$$p_\chi = \sum_i Tr(\rho P_i) \times Tr(\pi_\chi \frac{UP_i\rho P_i U^*}{p_i}) + \sum_j p'_j Tr(\pi_\chi \frac{VP'_j\rho P'_j U^*}{p'_j})$$

$$p_\chi = Tr(\pi_\chi F(\rho)).$$

F est donc compatible avec la notion de mesure.

Revenons aux boucles.

On pose :

- $\rho_0 = \rho$,
- $\rho_{n+1} = \sum_{i \in I} P_i \rho_n P_i + \sum_{j \in J} UP'_j \rho_n P'_j U^*$,
- $\tilde{\rho}_n = \rho_n - \sum_{(j_1, \dots, j_n) \in J^n} UP'_{j_1} \dots UP'_{j_n} \rho_0 P'_{j_1} U^* \dots P'_{j_n} U^*$.

C'est-à-dire que ρ_n représente la répartition de probabilité en fonction de la mesure de O du résultat de l'algorithme après n étapes. (On est entre $\rho = U\rho U^*$ et $b = \text{mesure de } O$.) Quant à $\tilde{\rho}_n$, c'est la partie de ρ_n pour laquelle l'algorithme a déjà terminé : c'est la répartition de probabilité du résultat à la fin de l'étape n .

Montrons que $\tilde{\rho}_n$ converge vers une limite $\tilde{\rho}$ qui dépend linéairement de ρ .

Pour cela, démontrons le lemme suivant :

Lemme A.1 :

Pour tout $n > 0$, on a

$$\tilde{\rho}_n = \sum_{i \in I} P_i \rho_0 P_i + \sum_{k=1}^{n-1} \sum_{i \in I, j_1, \dots, j_k \in J^k} P_i UP'_{j_k} \dots UP'_{j_1} \rho_0 P'_{j_1} U^* \dots P'_{j_k} U^* P_i \quad (5)$$

Preuve : Montrons par récurrence sur $n > 0$, que

$$\rho_n = \sum_{i \in I} P_i \rho_0 P_i + \sum_{k=1}^{n-1} \sum_{i \in I, j \in J^k} P_i UP'_{j_k} \dots UP'_{j_1} \rho_0 (P'_{j_1} U^* \dots P'_{j_k} U^* P_i + \sum_{j \in J^n} UP'_{j_n} \dots UP'_{j_1} \rho_0 P'_{j_1} U^* \dots P'_{j_n} U^*)$$

Initialisation : $n = 1$

Par définition,

$$\rho_1 = \sum_{i \in I} P_i \rho_0 P_i + \sum_{j \in J} (UP'_j)^n \rho_0 (P'_j U^*)^n.$$

Récurrence $n \rightarrow n + 1$:

$$\rho_{n+1} = \sum_{i \in I} P_i \rho_n P_i + \sum_{j \in J} UP'_j \rho_n P'_j U^*$$

Or, pour tout $i, i' \in I, j, j' \in J$, on a $P_i P_{i'} = \delta_{i,i'} P_i$, $P'_j P'_{j'} = \delta_{j,j'} P'_j$ et $P_i P'_j = 0$, on en déduit :

$$\begin{aligned} P_i \rho_n P_i &= P_i \rho_0 P_i + \sum_{k=1}^{n-1} \sum_{j \in J^k} P_i (UP'_{j_k} \dots UP'_{j_1}) \rho_0 (P'_{j_1} U^* \dots P'_{j_k} U^*) P_i + \sum_{j \in J^n} P_i (UP'_{j_n} \dots UP'_{j_1}) \rho_0 (P'_{j_1} U^* \dots P'_{j_n} U^*) P_i \\ &= P_i \rho_0 P_i + \sum_{k=1}^n \sum_{j \in J^k} P_i (UP'_{j_k} \dots UP'_{j_1}) \rho_0 (P'_{j_1} U^* \dots P'_{j_k} U^*) P_i \end{aligned}$$

et

$$\sum_{j \in J} UP'_j \rho_n P'_j U^* = \sum_{j \in J^{n+1}} UP'_{j_{n+1}} \dots UP'_{j_1} \rho_0 P'_{j_1} U^* \dots P'_{j_{n+1}} U^*$$

d'où le résultat.

On en déduit :

$$\tilde{\rho}_n = \sum_{i \in I} P_i \rho_0 P_i + \sum_{k=1}^{n-1} \sum_{i \in I, j_1, \dots, j_k \in J^k} P_i UP'_{j_k} \dots UP'_{j_1} \rho_0 P'_{j_1} U^* \dots P'_{j_k} U^* P_i$$

★

On voit alors que $\tilde{\rho}_n$ est croissante au sens de l'ordre sur les matrices positives. De plus, comme $Tr(\rho_{n+1}) = Tr(\rho_n)$, on a $Tr(\tilde{\rho}_n) \leq Tr(\rho_n) = Tr(\rho_0)$ donc la suite est bornée. Elle converge à extraction près, mais comme elle est croissante elle converge vers une limite $\tilde{\rho}$.

Enfin, comme ρ_n dépend linéairement de ρ_{n-1} , par récurrence, ρ_n dépend linéairement de ρ , et donc $\tilde{\rho}_n$ également. On en déduit que $\tilde{\rho}$ dépend linéairement de ρ . Il existe donc une application linéaire F telle que $\tilde{\rho} = F(\rho)$. Notons que comme, $\rho \mapsto \tilde{\rho}_n$ est superpositive (elle se met sous la forme $\rho \mapsto \sum_{\lambda \in \Lambda} V_\lambda \rho V_\lambda^*$), F est également superpositive.

On utilise F pour modéliser l'algorithme.

A.2.2 Cas d'une boucle qui ne termine pas

Commentons la valeur de la trace de $\tilde{\rho}_n$.

La probabilité pour que l'algorithme effectue exactement n calculs de $\rho \mapsto U\rho U^*$ est :

$$p_n = \sum_{i \in I} \sum_{j_1, \dots, j_n \in J^n} Tr(P_i UP'_{j_n} \dots UP'_{j_1} \rho_0 P'_{j_1} U^* \dots P'_{j_n} U^* P_i)$$

Autrement dit, la probabilité pour que l'algorithme termine en moins de n calculs de H_1 est :

$$P_{\leq n} = \sum_{k=0}^n p_n = Tr(\tilde{\rho}_{n+1})$$

Finalement, la trace de $\tilde{\rho}$ correspond à la probabilité qu'il existe n tel que l'algorithme s'arrête à l'étape n .

Supposons que la probabilité pour que l'algorithme ne termine pas soit supérieure à ε , c'est-à-dire que pour tout n , la probabilité pour que l'algorithme ne termine pas avant l'étape n soit supérieure à ε , autrement dit :

$$Tr(\tilde{\rho}_n) \leq 1 - \varepsilon$$

alors $Tr(\tilde{\rho}) \leq 1 - \varepsilon$.

On autorise donc F à faire diminuer la trace des opérateurs.

Un exemple de boucle qui ne termine pas

Cas simple, il existe un indice j_0 tel que H_1 et P'_{j_0} commute.

On a :

$$Tr(\rho_n - \tilde{\rho}_n) = \sum_{(j_1, \dots, j_n) \in J^n} Tr(UP'_{j_n} \dots UP'_{j_1} \rho_0 P'_{j_1} U^* \dots P'_{j_n} U^*)$$

$$Tr(\rho_n - \tilde{\rho}_n) \geq Tr((UP'_{j_0})^n \rho (P'_{j_0} U^*)^n)$$

Comme H_1 et P'_{j_0} commutent et que $(P'_{j_0})^n = P'_{j_0}$,

$$Tr(\rho_n - \tilde{\rho}_n) \geq Tr(U^n P'_{j_0} \rho P'_{j_0} (U^*)^n)$$

et comme H_1 est unitaire,

$$Tr(\rho_n - \tilde{\rho}_n) \geq Tr(P'_{j_0} \rho P'_{j_0}).$$

Finalement, pour un choix d'entrée tel que $Tr(P'_{j_0} \rho) \geq \varepsilon Tr(\rho)$ avec $\varepsilon > 1$, on a

$$Tr(F(\rho)) \leq (1 - \varepsilon) Tr(\rho).$$

B Bibliographie

Références

- [1] Florian Mintert; Andre R. R. Carvalho; Marek Kus; Andreas Buchleitner, *Mesures and dynamics of entangled states*, (Physics Report, 415, 207 (2005)).
- [2] Michael A. Nielsen; Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.
- [3] Pierre-Louis Curien, *Introduction to linear logic and ludics, part 1 & 2*, (dans *Advances in Mathematics (China)* 34, 5 (2005) 513-544, en 2005).
- [4] Thomas Ehrhard, *Finiteness spaces*, (dans *Mathematical Structures in Computer Science (2005)*, 15 :4 :615-646 Cambridge University Press).
- [5] Vincent Danos; Thomas Ehrhard, *On probabilistic coherence spaces*, (2008, publié sur HAL - CCSD).
- [6] Jean-Yves Girard, *Le point aveugle, tomes 1 & 2*, Hermann, 2006.
- [7] Jean-Yves Girard, *Du pourquoi au comment : la théorie de la démonstration de 1950 à nos jours*, (dans *Les mathématiques 1950-2000*, ed. Pier, pp. 515-545, Birkhauser, en 2000).
- [8] Jean-Yves Girard, *Between logic and quantics : a tract*, (dans *Linear logic in computer science*, eds Ehrhard, Girard, Ruet and Scott, Cambridge University Press, en 2004).
- [9] M. Horodecki; P Horodecki; R. Horodecki, *Mixed-state entanglement and quantum communication*, (dans « *Quantum Information : An Introduction to Basic Theoretical Concepts* », 2008).
- [10] L. Landau; E. Lifchitz, *Mécanique quantique : théorie non-relativiste, cours de physique théorique 3*, Mir, 1967.
- [11] Thierry Lévy, *Le critère de séparabilité de la famille Horodecki*, (2003).
- [12] Paul-André Melliès, *Categorical semantics of linear logic*, (à paraître).
- [13] Thierry Paul, *From quantum to classical by letting the dimension diverge*, (preprint).
- [14] R.F. Blute; Prakash Panangaden; R.A.G Seely, *Fock space : A model of linear exponential types*, (1993, preprint).
- [15] Peter Selinger, *Towards a quantum programming language*, (2003, dans *Mathematical Structures in Computer Science* 14(4) :527-586).
- [16] Bernd Thaller, *The Dirac equation*, Springer, 1992.
- [17] Jamie Vicary, *A categorical framework for the quantum harmonic oscillator*, (*International Journal of Theoretical Physics*, Volume 47, Number 12 / décembre 2008).
- [18] Martin B. Plenio; Shashank Virmani, *An introduction to entanglement measures*, (*Quant. Inf. Comp.* 7, 1 (2007)).