

Canaux quantiques et théorème de Choi-Kraus

Quelques bases du formalisme de la théorie quantique de l'information

Félix Faisant

Mémoire de L3 encadré par Amaury Freslon

18 mai 2019

Résumé

Après avoir présenté les postulats de la mécanique quantique ainsi que les bases du formalisme tensoriel, on introduit la notion de canal quantique en dimension finie, et on justifie, par le théorème de décomposition de Choi-Kraus, le choix de l'identifier aux *transformations complètement positives préservant la trace*. On prend soin de développer les détails mathématiques. Regardant les postulats, quelques intuitions et justifications sont données.

1 Contexte et postulats

Parmi toutes les bizarreries de la physique quantique, la plus déroutante est sans doute le comportement de ce que l'on appelle *information*. Si l'étude de l'information quantique n'est qu'une façon de voir la physique quantique, elle touche aussi bien les fondamentaux de la mécanique quantique et de ses interprétations (rôle de la mesure, théorie de la décohérence, déterminisme et causalité) que les applications pratiques (communication et informatique quantique). Ce sont des domaines en pleine effervescence.

On ne discutera ici que d'un bout du formalisme mathématique de la théorie quantique de l'information, à savoir les **canaux quantiques** de dimension finie et leur couplage (formalisé grâce à l'algèbre tensorielle), les opérateurs **complètement positifs**, et le **théorème de Choi-Kraus**. Ce mémoire se base sur les notes du cours *Intrication et Non-localité* de Vern Paulsen [PM990, 2016].

1.1 Postulats de la mécanique quantique : états et mesure

On rappelle les postulats de la mécanique quantique (dans l'interprétation de Born) puis on donne les postulats dans leur forme plus générale, c'est à dire en prenant en compte les *mélanges statistiques d'états* et l'évolution non unitaire. Pour une justification et une discussion approfondie de ces postulats, on renvoie à tout manuel de mécanique quantique adoptant ce système de postulats, par exemple [Le Bellac, ch. 4 et § 11.4.7] ou [Aslangul, ch. 12].

Axiome. *Un système quantique est représenté par un espace de Hilbert $(\mathcal{H}, \langle \cdot | \cdot \rangle)$. L'état du système est représenté par vecteur $\psi \in \mathcal{H}$ unitaire : $\|\psi\| = \langle \psi | \psi \rangle = 1$. Pour anticiper sur les mélanges statistiques, on appelle un tel état un **état pur**. On note $\mathcal{H}_{\text{unit}}$ l'ensemble des vecteurs unitaires.*

En mécanique quantique ondulatoire, $\mathcal{H} = L^2(\mathbb{R}^3)$ muni du produit hermitien usuel, et ψ est appelé la fonction d'onde du système étudié (par exemple une particule) : si l'on dispose d'un appareil mesurant la position du système, la fonction $x \mapsto |\psi(x)|^2$ est la densité de probabilité d'observer le système en x . Il est alors nécessaire d'imposer que $\langle \psi | \psi \rangle = \int |\psi|^2 = 1$ pour obtenir une densité de probabilité. On note que comme la mécanique ondulatoire est *linéaire* (« principe de superposition ») et nécessite $\mathbb{C}$ (équation de Schrödinger et interférences), il est naturel de se placer dans un espace de Hilbert. Ici, comme souvent en théorie quantique de l'information, *on se limite à des espaces de dimension finie*.

Axiome. (Postulat historique de Born)

Si $\phi \in \mathcal{H}_{\text{unit}}$ est un état pur, et si l'on dispose d'un appareil effectuant une telle mesure, pour tout système représenté par un état pur $\psi \in \mathcal{H}_{\text{unit}}$, la probabilité de mesurer le système dans l'état ϕ est

$$p(\psi \rightsquigarrow \phi) = |\langle \phi | \psi \rangle|^2 \quad (1)$$

et, immédiatement après l'observation, le système se trouve dans l'état mesuré ϕ .

Si l'on reprend l'exemple de $\mathcal{H} = L^2(\mathbb{R}^3)$ représentant une particule, ainsi qu'une boîte $B \subset \mathbb{R}^3$ et de l'état $\phi = \frac{\mathbb{1}_B}{\text{Volume}(B)}$, l'appareil effectue la mesure de présence dans la boîte, et $p(\psi \rightsquigarrow \phi)$ est la probabilité que l'on observe l'état ψ dans la boîte. Et immédiatement après cette observation, la particule est dans l'état ϕ , que l'on interprète usuellement par le fait que la particule est présente dans la boîte avec une probabilité uniforme. C'est ainsi que l'on nomme « réduction du paquet d'onde » le deuxième point¹. Nous n'en aurons pas usage ici, mais il est mentionné car la résolution de ce problème est (pour simplifier) une des raisons d'être de la théorie de la décohérence. Une partie de la communauté cherche en effet à modifier et *démontrer* cet axiome dans un cadre plus général.

Si la notion d'état pur est utile pour concevoir des sujets d'examen et idéaliser des situations, on ne sait jamais en réalité dans quel état un système est. Pour deux raisons : il est rare de préparer ou de disposer d'états purs, et les systèmes sont toujours en interaction avec un environnement que l'on ne maîtrise pas. Il est alors nécessaire de décrire de façon probabiliste (on dit *statistique* pour différencier, à tort ou à raison, avec le processus de mesure, lui aussi probabiliste) l'état d'un système : on parle de **mélange d'états**.

Commençons par une remarque : si l'on pose l'état $\psi' = e^{i\theta}\psi$ (changement de phase globale), on obtient

$$p(\psi' \rightsquigarrow \phi) = |\langle \phi | \psi' \rangle|^2 = |e^{i\theta} \langle \phi | \psi \rangle|^2 = |\langle \phi | \psi \rangle|^2 = p(\psi \rightsquigarrow \phi)$$

et ce pour tout état ϕ . étant donné que *seules les probabilités sont accessibles par l'expérience*, on en déduit que ψ' représente le même état. Si l'on pose alors l'opérateur $P_\psi = \psi\psi^*$, où $\psi^* := \langle \psi | \cdot \rangle$ est le dual hermitien de ψ , on remarque que $P_{\psi'} = \psi'\psi'^* = e^{i\theta}\psi e^{-i\theta}\psi^* = \psi\psi^* = P_\psi$: cet opérateur est bien *invariant par changement de phase globale*. Et surtout, on retrouve $p(\psi \rightsquigarrow \phi)$ à partir de P_ψ :

$$\text{tr}(P_\phi P_\psi) = \text{tr}(\phi\phi^*\psi\psi^*) = \text{tr}(\psi^*\phi\phi^*\psi) = \text{tr}(\langle \phi | \psi \rangle \langle \psi | \phi \rangle) = \langle \phi | \psi \rangle \langle \psi | \phi \rangle = |\langle \phi | \psi \rangle|^2 = p(\psi \rightsquigarrow \phi)$$

en utilisant l'identité de trace². On n'a donc rien perdu au change en passant de ψ à P_ψ .

Vérifions enfin quelques propriétés importantes de cet opérateur :

- P_ψ est hermitien (ou auto-adjoint) : $P_\psi^* = (\psi\psi^*)^* = \psi^{**}\psi^* = \psi\psi^* = P_\psi$.
- P_ψ est positif : $\forall \chi \in \mathcal{H}, \langle \chi | P_\psi \chi \rangle = \langle \chi | \psi\psi^* \chi \rangle = \langle \chi | \psi \rangle \langle \psi | \chi \rangle = \langle \psi | \chi \rangle \langle \chi | \psi \rangle = |\langle \psi | \chi \rangle|^2 \geq 0$
- P_ψ est de trace unité : $\text{tr}(P_\psi) = \text{tr}(\psi\psi^*) = \text{tr}(\psi^*\psi) = \langle \psi | \psi \rangle = 1$.
- P_ψ est un projecteur : $P_\psi^2 = \psi\psi^*\psi\psi^* = \psi\langle \psi | \psi \rangle\psi^* = 1\psi\psi^* = P_\psi$.

1. Cette projection instantanée défie nos intuitions de continuité et est sujette à controverse depuis la naissance de la mécanique quantique. La « réduction du paquet d'onde » (*collapse*) est toutefois nécessaire pour assurer la cohérence logique de la théorie en l'état [Aslangul, §12.1.4], et ses conséquences sont vérifiées par l'expérience (effet Zénon quantique...)

2. On se permet quelques raccourcis dans les notations, en notant de manière multiplicative à la fois la composition d'opérateurs et la multiplication scalaire. Si l'on veut être très explicite, on peut écrire que $P_\psi = \psi\psi^* = \langle \psi | \cdot \rangle \psi$, puis

$$\text{tr}(P_\phi P_\psi) = \text{tr} \left((\langle \phi | \cdot \rangle \phi) \circ (\langle \psi | \cdot \rangle \psi) \right) = \text{tr} \left(\langle \phi | \langle \psi | \cdot \rangle \psi \phi \right) = \text{tr} (\langle \psi | \cdot \rangle \langle \phi | \psi \rangle \phi) = \langle \phi | \psi \rangle \text{tr} (\langle \psi | \cdot \rangle \phi)$$

puis comme $\langle \psi | \cdot \rangle \phi = (\lambda \mapsto \lambda \phi) \circ \langle \psi | \cdot \rangle$, on a par l'identité de trace en (*) :

$$\text{tr} (\langle \psi | \cdot \rangle \phi) = \text{tr} ((\lambda \mapsto \lambda \phi) \circ \langle \psi | \cdot \rangle) \stackrel{(*)}{=} \text{tr} (\langle \psi | \cdot \rangle \circ (\lambda \mapsto \lambda \phi)) = \text{tr} (\lambda \mapsto \langle \psi | \lambda \phi \rangle) = \text{tr} (\lambda \mapsto \lambda \langle \psi | \phi \rangle) = \langle \psi | \phi \rangle$$

donc $\text{tr}(P_\phi P_\psi) = \langle \phi | \psi \rangle \text{tr} (\langle \psi | \cdot \rangle \phi) = \langle \phi | \psi \rangle \langle \psi | \phi \rangle = |\langle \phi | \psi \rangle|^2$. On se permettra ce genre de raccourcis dans la suite.

On rappelle les caractérisations de la positivité [Conway, ch. VIII, th. 3.6 & 3.8] d'un opérateur hermitien de la C*-algèbre $\mathcal{L}(\mathcal{H})$:

$$\begin{aligned} A \text{ positif} &\iff \forall x \in \mathcal{H}, \langle x|Ax \rangle \geq 0 \quad (\text{la forme hermitienne associée est positive}) \\ &\iff \text{Sp}(A) \subset \mathbb{R}_+ \\ &\iff \exists V \in \mathcal{L}(\mathcal{H}) : A = V^*V \\ &\iff \exists W \in \mathcal{L}(\mathcal{H}) \text{ hermitien} : A = W^2 \end{aligned}$$

équivalences prouvées par décomposition spectrale. On note $\mathcal{L}^+(\mathcal{H})$ l'ensemble des opérateurs hermitiens positifs sur $\mathcal{H}$, et $\mathcal{L}_{\text{tr } 1}^+(\mathcal{H}) = \{A \in \mathcal{L}^+(\mathcal{H}) : \text{tr}(A) = 1\}$ ceux de trace unité.

Sautons sans plus attendre aux mélanges statistiques. Donnons nous une famille d'états associés à une probabilité $(\psi_\ell, \rho_\ell)_{1 \leq \ell \leq r} \in (\mathcal{H}_{\text{unit}} \times [0, 1])^r$, telle que $\sum_\ell \rho_\ell = 1$. On pose alors

$$P = \sum_\ell \rho_\ell P_{\psi_\ell} = \sum_\ell \rho_\ell \psi_\ell \psi_\ell^* \quad (2)$$

l'opérateur associé au **mélange propre** $(\psi_\ell, \rho_\ell)_\ell$, somme pondérée de projecteurs, décrivant un système qui est dans l'état ψ_ℓ avec une probabilité ρ_ℓ . On vérifie alors que P est positif :

$$\forall \chi \in \mathcal{H}, \quad \langle \chi | P \chi \rangle = \left\langle \chi \left| \sum_\ell \rho_\ell \psi_\ell \psi_\ell^* \chi \right. \right\rangle = \sum_\ell \rho_\ell \langle \chi | \psi_\ell \psi_\ell^* \chi \rangle = \sum_\ell \rho_\ell \overbrace{|\langle \psi_\ell | \chi \rangle|^2}^{\geq 0} \geq 0$$

De même, puisque $\text{tr}(P_{\psi_\ell}) = \text{tr}(\psi_\ell \psi_\ell^*) = 1$, cet opérateur est de trace $\text{tr}(P) = 1$. Enfin, la formule ci-dessus $\text{tr}(P_\phi P_\psi) = p(\psi \rightsquigarrow \phi)$ se généralise aux mélanges propres :

$$\text{tr}(P_\phi P) = \sum_\ell \rho_\ell \text{tr}(P_\phi P_{\psi_\ell}) = \sum_\ell \rho_\ell |\langle \phi | \psi_\ell \rangle|^2 = \sum_\ell \rho_\ell p(\psi_\ell \rightsquigarrow \phi) \quad (3)$$

ce qui est ce que l'on attendait : la probabilité $p(P \rightsquigarrow \phi) := \text{tr}(P_\phi P)$ d'observer le système dans l'état pur ϕ est la somme des $p(\psi_\ell \rightsquigarrow \phi)$, pondérée par la probabilité ρ_ℓ que le système fut dans l'état ψ_ℓ .

On généralise ainsi les états purs aux mélanges d'états :

Axiome 1. *Un système quantique est représenté par un espace de Hilbert $(\mathcal{H}, \langle \cdot | \cdot \rangle)$. L'état du système est représenté par un **opérateur statistique** $P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H})$, c'est-à-dire hermitien positif de trace unité.*

À un **mélange propre** $(\psi_\ell, \rho_\ell)_{1 \leq \ell \leq r} \in (\mathcal{H}_{\text{unit}} \times \mathbb{R}_+)^r$ où $\sum_\ell \rho_\ell = 1$, on associe l'opérateur statistique

$$P = \sum_{\ell=1}^r \rho_\ell P_{\psi_\ell} \quad (4)$$

Un opérateur statistique est parfois appelé *matrice de densité*. À noter que si les mélanges propres donnent naturellement un opérateur statistique, il n'y a aucune raison qu'un tel opérateur s'écrive sous la forme (2) dans une base $(\psi_i)_i$ fixée. C'est le cas d'un *mélange impropre*, qui représente un sous-système couplé d'un système plus grand, par exemple un système étudié, que l'on maîtrise, couplé avec son environnement, que l'on ne maîtrise pas. On détaillera cette notion de couplage dans la suite. Toutefois, puisque P est hermitien, par le théorème spectral, il existe une base orthonormale $(\varphi_i)_i$ dans laquelle sa matrice $\text{diag}(p_i)_i$ soit diagonale, c'est-à-dire $P = \sum_i \rho_i \varphi_i \varphi_i^*$. Alors, puisque $\text{tr}(P) = 1$, $\sum_i \rho_i = 1$. On garde toutefois à l'esprit que $(\psi_i, \rho_i)_i$ n'est pas le mélange propre de P en général³.

On généralise de même le postulat de Born aux mélanges d'états :

3. La base dans laquelle on travaille est fixée lorsque le dispositif expérimental est fixé. Néanmoins, en pratique, rien ne distingue un mélange propre d'un mélange impropre. C'est surtout une différence conceptuelle, qui est pourtant fondamentale pour la théorie de la mesure [Le Bellac, p.393, p.429].

Axiome. Si $\phi \in \mathcal{H}$ est un état pur ($\|\phi\| = 1$), et si l'on dispose d'un appareil effectuant une telle mesure, pour tout système représenté par un mélange d'état $P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H})$, la probabilité de mesurer le système dans l'état ϕ est (toujours avec P_ϕ le projecteur sur ϕ) :

$$p(P \rightsquigarrow \phi) = \text{tr}(P_\phi P) \quad (5)$$

et, immédiatement après l'observation, le système se trouve dans l'état mesuré ϕ .

On remarque que puisque $P_\phi = P_\phi^2 = P_\phi P_\phi^*$, on peut écrire $p(P \rightsquigarrow \phi) = \text{tr}(P_\phi P P_\phi^*)$. De plus, l'état après mesure est ϕ , c'est-à-dire P_ϕ sous forme d'opérateur. Si l'on complète la famille (ϕ) en une base orthogonale, on a dans cette base $\text{mat}(P_\phi) = [\mathbb{1}_{i,1} \mathbb{1}_{j,1}]_{i,j}$ et $\text{mat}(P) = [\rho_{i,j}]_{i,j}$ et on remarque alors que $\text{mat}(P_\phi P P_\phi^*) = [\rho_{1,1} \mathbb{1}_{i,1} \mathbb{1}_{j,1}]_{i,j} = \text{mat}(\rho_{1,1} P_\phi)$ et donc $p(P \rightsquigarrow \phi) = \text{tr}(P_\phi P P_\phi^*) = \rho_{1,1}$. Donc immédiatement après mesure (et si $p(P \rightsquigarrow \phi) \neq 0$, sinon ça n'a pas d'intérêt) $P_{\text{post}} = P_\phi = \frac{P_\phi P P_\phi^*}{\text{tr}(P_\phi P P_\phi^*)}$.

Ce postulat n'est que temporaire, il ne sert qu'à introduire l'axiomatisation suivante d'une mesure, beaucoup plus générale, que l'on peut déduire des remarques que l'on vient de faire :

Axiome 2. Une mesure d'un système quantique dont les issues sont indexées par $k \in \llbracket 1, m \rrbracket$ est représentée par une famille d'opérateurs linéaires, que l'on appelle un **système de mesure**,

$$(M_k : \mathcal{H}_s \longrightarrow \mathcal{H}_o)_{1 \leq k \leq m} \in \mathcal{L}(\mathcal{H}_s, \mathcal{H}_o)^m$$

avec $\mathcal{H}_s$ l'espace des états avant la mesure (state space) et $\mathcal{H}_o$ l'espace des états après la mesure (outcome space), tels que, pour un mélange d'état $P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_s)$, la probabilité d'observer l'issue n° k est

$$p_k(P) = \text{tr}(M_k P M_k^*) \quad \text{avec} \quad \sum_{k=1}^m p_k(P) = 1 \quad (6)$$

En particulier, si l'on a un état pur $\psi \in \mathcal{H}_s$, alors $P = P_\psi$ et $p_k = \text{tr}(M_k P_\psi M_k^*) = \text{tr}(M_k \psi \psi^* M_k^*) = \text{tr}((M_k \psi)(M_k \psi)^*) = \langle M_k \psi | M_k \psi \rangle$ donc la probabilité d'observer l'issue n° k est :

$$p_k = \|M_k \psi\|^2 \quad (7)$$

Donnons tout de suite une condition plus pratique pour que le système de mesure définisse bien une probabilité : $\forall \psi \in (\mathcal{H}_s)_{\text{unit}}$, on doit avoir

$$1 = \sum_{k=1}^m p_k(\psi) = \sum_{k=1}^m \langle M_k \psi | M_k \psi \rangle = \sum_{k=1}^m \langle \psi | M_k^* M_k \psi \rangle = \langle \psi | M \psi \rangle \quad \text{avec} \quad M = \sum_{k=1}^m M_k^* M_k$$

M étant clairement hermitien, on peut le diagonaliser dans une base orthonormale $(\varphi_i)_i$ dans laquelle $\text{mat}(M) = \text{diag}(\lambda_i)_i$. Alors $\forall i$, $1 = \langle \varphi_i | M \varphi_i \rangle = \langle \varphi_i | \lambda_i \varphi_i \rangle = \lambda_i \langle \varphi_i | \varphi_i \rangle = \lambda_i$, donc $\text{mat}(M) = 1$, donc $M = 1$ puisque l'identité commute avec les matrices de changement de base. Réciproquement, si l'on a $\sum_{k=1}^m M_k^* M_k = 1$, alors $\forall P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_s)$,

$$\sum_{k=1}^m p_k = \sum_{k=1}^m \text{tr}(M_k P M_k^*) = \sum_{k=1}^m \text{tr}(M_k^* M_k P) = \text{tr}\left(\sum_{k=1}^m M_k^* M_k P\right) = \text{tr}(1 P) = \text{tr}(P) = 1$$

Ainsi,

$$(M_k : \mathcal{H}_s \longrightarrow \mathcal{H}_o)_{1 \leq k \leq m} \text{ système de mesure} \iff \sum_{k=1}^m M_k^* M_k = \mathbb{1}_{\mathcal{H}_s} \quad (8)$$

La définition d'un système de mesure que l'on a donnée est la plus générale ayant un sens (c'est-à-dire définissant une probabilité) définie sur un tel ensemble d'issues⁴, tout du moins en dimension finie.

4. Dans ce texte, on se place dans la *représentation de Schrödinger* : cela signifie que les opérateurs de mesure sont **fixés**, et ce sont les vecteurs d'états (ou les mélanges statistiques) qui évoluent. Cela semble évident, mais dans la *représentation de Heisenberg*, qui décrit de façon équivalente une évolution quantique, c'est l'inverse.

Mais souvent, les systèmes de mesures étudiés sont des P.O.M.V. (*positive-operator valued measure*), c'est-à-dire une famille $(F_k)_k \in \mathcal{L}^+(\mathcal{H})$ d'opérateurs positifs tels que $\sum_k F_k = 1$, que l'on peut alors décomposer (de façon non unique) en $F_k = M_k^* M_k$. Souvent même, dans les cours introductifs de mécanique quantique, on étudie un seul opérateur hermitien A , alors appelé **observable** et diagonalisable, et on énonce le postulat précédent en terme de spectre (réel) et de projection sur les espaces propres.

On peut regarder le cas particulier où système de mesure est l'observation d'états purs d'une base orthonormale $(\psi_i)_{1 \leq i \leq n}$, c'est-à-dire $M_i = \psi_i \psi_i^* = M_i^*$. La probabilité de mesurer le système (représenté par le mélange d'état $P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_s)$) dans l'état ψ_i est alors, grâce à la formule de la trace,

$$p_i = \text{tr}(\psi_i \psi_i^* P \psi_i \psi_i^*) = \text{tr}(\psi_i \psi_i^* P) = \text{tr}(P \psi_i \psi_i^*) \quad (9)$$

ce qui est bien ce que l'on attendait (voir (5)).

Enfin, on peut regarder le cas où P représente une mélange propre $(\psi_\ell, \rho_\ell)_{1 \leq \ell \leq r} \in (\mathcal{H}_{\text{unit}} \times \mathbb{R}_+)^r$: la probabilité d'observer l'issue n° k est donnée par

$$p_k = \text{tr}(M_k P M_k^*) = \text{tr}\left(M_k \sum_{\ell} \rho_\ell P \psi_\ell \psi_\ell^* M_k^*\right) = \sum_{\ell} \rho_\ell \text{tr}(M_k P \psi_\ell \psi_\ell^* M_k^*) \stackrel{(7)}{=} \sum_{\ell} \rho_\ell \|M_k \psi_\ell\|^2 \quad (10)$$

qui est la somme pondérée par les coefficients de mélange ρ_ℓ des probabilités (7) d'observer cette issue pour l'état pur ψ_ℓ , résultat intuitif que l'on aurait pu utiliser pour déterminer la formule (6) générale [PM990, th. 3.9]. On remarque ici que, si deux mélanges propres $(\psi_\ell, \rho_\ell)_\ell, (\psi'_\ell, \rho'_\ell)_\ell$ ont le même opérateur P , puisque *seules les probabilités $p_k(P)$ sont accessibles par l'expérience*, aucun système de mesure ne peut les distinguer. On peut aisément trouver des mélanges propres distincts ayant le même opérateur statistique, cela justifie donc le formalisme de l'opérateur statistique.

On énonce le postulat d'évolution de l'état après observation par le système de mesure :

Axiome 3. *Immédiatement après l'observation de l'issue n° k , le système se trouve dans l'état*

$$P_{\text{post},k} = \frac{M_k P M_k^*}{p_k} = \frac{M_k P M_k^*}{\text{tr}(M_k P M_k^*)} \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_o) \quad (11)$$

On note que $P_{\text{post},k}$, qui n'est rien d'autre qu'une projection normalisée, est de trace $\text{tr}(P_{\text{post},k}) = 1$. De plus, $\forall \chi \in \mathcal{H}$, $\langle \chi | P_{\text{post},k} \chi \rangle = p_k^{-1} \chi^* M_k P M_k^* \chi = p_k^{-1} (M_k^* \chi)^* P M_k^* \chi = p_k^{-1} \langle \chi' | P \chi' \rangle \geq 0$ avec $\chi' = M_k^* \chi$, donc $P_{\text{post},k}$ est encore positif. C'est donc bien un opérateur statistique.

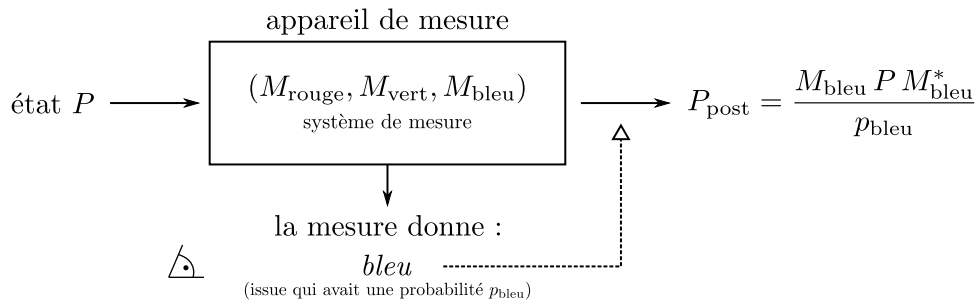


FIGURE 1 – Système de mesure et état individuel après observation de l'issue.

Mais quid du résultat d'une mesure lorsque l'on a *pas* accès à l'issue de l'observation ? Tout ce que l'on peut dire, c'est que l'on a une probabilité p_k que l'issue n° k ait été « observée »⁵. On a donc affaire à

5. La formulation « que l'issue n° k ait été observée » peut être tout à fait remise en cause, surtout au vu du mélange statistique que l'on obtient après. Si l'on a pas accès à l'observation, c'est-à-dire isolé du système de mesure, est-on en droit de dire que l'« observation » a réellement eu lieu ? On pourrait très bien dire que le système de mesure est en superposition d'état. On touche ici aux questions profondes, et ouvertes, d'interprétation de la mécanique quantique.

un mélange propre $(P_{\text{post},k}, p_k)_{1 \leq k \leq m}$, c'est-à-dire à l'opérateur statistique (cf. (4))

$$P_{\text{post}} = \sum_{k=1}^m p_k P_{\text{post},k} = \sum_{k=1}^m p_k \frac{M_k P M_k^*}{p_k} = \sum_{k=1}^m M_k P M_k^* \quad (12)$$

Puisque $\sum_{k=1}^m p_k = 1$ et que $P_{\text{post},k} \in \mathcal{L}_{\text{tr}1}^+(\mathcal{H}_o)$, on a bien évidemment que $P_{\text{post}} \in \mathcal{L}_{\text{tr}1}^+(\mathcal{H}_o)$.

Comme on le verra, toute évolution quantique, par exemple la transmission d'un photon dans une fibre optique, peut être représenté (de façon non unique) comme un système de mesure, sans que l'on puisse parler d'issue de mesure car on ne connaît pas l'état microscopique de la fibre optique après transmission. La seule forme raisonnable de l'état après « mesure » est alors celle d'un mélange d'états.

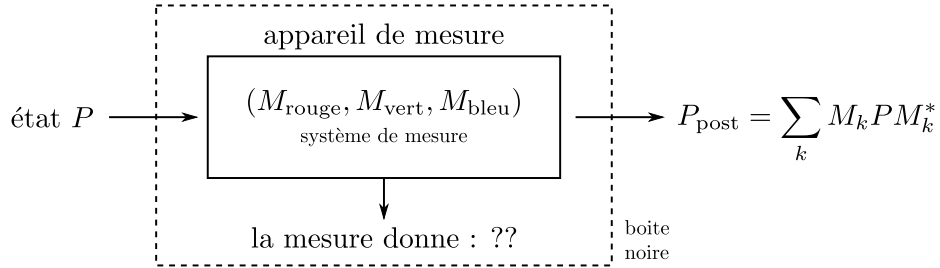


FIGURE 2 – Système de mesure et état individuel après mesure, d'issue inconnue, donnant un mélange d'états.

Une autre situation dans laquelle la forme (12) prend tout son sens est lorsque l'on regarde non pas un état du système, mais un (grand) ensemble de réalisations de la mesure (par exemple lorsque l'on étudie une *population* de photons, d'atomes...). En effet, même si la mesure sur chaque état individuel donne un état de la forme $P_{\text{post},k}$, statistiquement, sur un grand nombre de réalisations, on obtient P_{post} en moyenne.

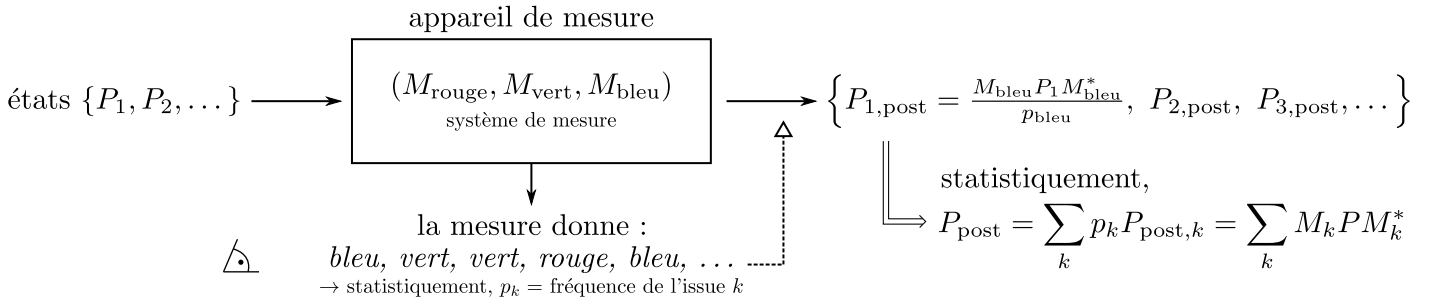


FIGURE 3 – Système de mesure et statistique sur un ensemble de réalisation de mesures donnant un mélange d'états.

1.2 Évolution et opérations quantiques

Le formalisme mathématique que l'on va maintenant présenter a pour but de décrire les *systèmes quantiques ouverts*. Désormais standard en théorie quantique de l'information, il est principalement dû à Karl Kraus [1983] et se base sur des travaux de Man-Duen Choi [1975] et de Stinespring. Parmi les différents formalismes établis, il a l'avantage de ne nécessiter que les opérateurs statistiques pour décrire un système et son évolution.

Mentionnons tout d'abord que, lorsque le système considéré est *isolé* (n'interagissant pas avec l'environnement, en particulier en dehors de toute mesure), un état pur ψ évolue dans le temps selon l'équation de Schrödinger :

$$i\hbar \partial_t \psi(t) = H(t) \psi(t)$$

avec $H(t)$ le hamiltonien du système, qui est un opérateur hermitien imposé par la physique du système. Dans le cadre plus général des mélanges d'états, l'opérateur d'état $t \mapsto P(t)$ obéit à [Le Bellac, p.393]

$$i\hbar \partial_t P(t) = [P(t), H(t)]$$

avec $[\cdot, \cdot]$ le commutateur. Il est remarquable que l'on puisse réécrire cette évolution ainsi :

$$P(t) = U_t P_0 U_t^{-1} \quad \text{avec } U_t \text{ l'opérateur d'évolution de } t_0 \text{ à } t$$

opérateur hermitien unitaire (vérifiant $U_t^{-1} = U_t^*$) indépendant de l'état et vérifiant $i\hbar \partial_t U_t = H(t)U_t$ et $U_{t=0} = 1$. On parle alors d'évolution hamiltonienne, et plus généralement d'*évolution unitaire*.

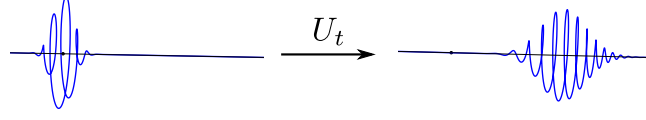


FIGURE 4 – Évolution hamiltonienne d'un paquet d'onde gaussien 1D.

Dans le cas particulier d'un état pur initial ψ_0 , on remarque que le système reste dans un état pur⁶ :

$$\psi(t) = U_t \psi_0$$

Mais lors d'une mesure, et plus généralement lorsque le système interagit avec son environnement (on parle de système *ouvert*), l'évolution $P \rightarrow P_{\text{post}}$ (11) n'est en général *pas* unitaire, et peut même nécessiter de changer d'espace. Pour généraliser l'évolution des états d'un système ouvert, on postule que :

Axiome 4. *Toute évolution d'un système quantique est représentée par un opérateur linéaire*

$$\Phi : \mathcal{L}(\mathcal{H}_s) \longrightarrow \mathcal{L}(\mathcal{H}_o)$$

tel que tout opérateur statistique de $\mathcal{H}_s$ est envoyé sur un opérateur statistique de $\mathcal{H}_o$:

$$\forall P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_s), \quad \Phi(P) \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_o)$$

dit **opérateur d'évolution**⁷.

L'évolution hamiltonienne $t_0 \rightarrow t$ est donné par $\Phi_u : P \mapsto U_t P U_t^{-1}$ sur $\mathcal{H}_s = \mathcal{H}_o = \mathcal{H}$. On vérifie que $\forall P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H})$, $\text{tr}(\Phi_u(P)) = \text{tr}(U_t P U_t^{-1}) = \text{tr}(P U_t^{-1} U_t) = \text{tr}(P U_t^* U_t) = \text{tr}(P \mathbb{1}) = \text{tr}(P)$. De plus, $\Phi_u(P)$ est positif car $\forall x \in \mathcal{H}$, $\langle x | \Phi_u(P) x \rangle = \langle x | U_t P U_t^{-1} x \rangle = \langle x | P x \rangle \geq 0$ puisque un opérateur unitaire conserve le produit scalaire.

Si l'on effectue une mesure, représentée par un système de mesure $(M_k : \mathcal{H}_s \longrightarrow \mathcal{H}_o)_{1 \leq k \leq m}$, l'opérateur d'évolution associé à l'observation de l'issue n° k est donné par (cf. 11) :

$$\Phi_{m,k} : P \longmapsto \frac{M_k P M_k^*}{\text{tr}(M_k P M_k^*)} \quad (13)$$

et lorsque l'on ne connaît pas l'issue de la mesure, ou qu'on regarde un ensemble de réalisations de la mesure, l'évolution est donnée par (cf. 12) :

$$\Phi_m : P \longmapsto \sum_{k=1}^m M_k P M_k^* \quad (14)$$

pour lesquels on a déjà vérifié que les mélanges d'états sont envoyés sur des mélanges d'états.

Donnons une caractérisation plus pratique de cette propriété :

6. On dit alors qu'il n'y a pas décohérence de l'état

7. Terme non standard. On a choisi ici d'éviter de parler d'*opération quantique*. En effet, ce terme est parfois utilisé pour nommer notre opérateur d'évolution quantique, et parfois utilisé comme synonyme de *canal quantique*, qui, lui, doit être de plus complètement positif.

Théorème 1. (Opérateur d'évolution $\Leftrightarrow$ Transformation positive préservant la trace).

Soit $\Phi : \mathcal{L}(\mathcal{H}_1) \rightarrow \mathcal{L}(\mathcal{H}_2)$ décrivant une évolution quantique, c'est-à-dire envoyant les opérateurs statistiques sur des opérateurs statistiques. Alors :

- i. Φ est une **transformation positive** : $\forall A \in \mathcal{L}^+(\mathcal{H}_1)$ opérateur positif, $\Phi(A) \in \mathcal{L}^+(\mathcal{H}_2)$ positif
- ii. Φ préserve la trace : $\forall A \in \mathcal{L}(\mathcal{H}_1), \quad \text{tr}(\Phi(A)) = \text{tr}(A)$

La réciproque est vraie par définition. $\triangle$ Ne pas confondre la notion d'opérateur (hermitien) positif et celle de transformation positive, que l'on peut définir plus généralement comme une transformation de C^* -algèbre envoyant les éléments positifs de l'algèbre sur des éléments positifs.

Démonstration. On suppose que Φ envoie $\mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_1)$ dans $\mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_2)$.

Soit $A \in \mathcal{L}^+(\mathcal{H}_1)$ un opérateur hermitien positif.

Alors par le théorème spectral, A est diagonalisable, ses valeurs propres sont positives, et $\text{tr}(A) \geq 0$.

- Cas $\text{tr}(A) = 0$: Alors $\sum_{\lambda \in \text{Sp}(A)} \overset{\geq 0}{\lambda} = \text{tr}(A) = 0$ donc $\forall \lambda \in \text{Sp}(A), \lambda = 0$. Donc $A = 0$, donc $\Phi(A) = 0$ est l'opérateur nul, qui est positif. De plus, $\text{tr}(\Phi(A)) = 0 = \text{tr}(A)$.
- Cas $\text{tr}(A) > 0$: Alors $P := \text{tr}(A)^{-1} \cdot A$ est positif et de trace $\text{tr}(P) = 1$, donc $\Phi(P) \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_2)$, donc
 - $\Phi(P) = \Phi(\text{tr}(A)^{-1} A) = \text{tr}(A)^{-1} \Phi(A)$ est un opérateur positif, donc $\forall x \in \mathcal{H}_1, \langle x | \Phi(A) x \rangle = \underbrace{\text{tr}(A)}_{>0} \underbrace{\langle x | \Phi(P) x \rangle}_{\geq 0} \geq 0$ donc $\Phi(A)$ est encore positif.
 - $1 = \text{tr}(\Phi(P)) = \text{tr}\left(\frac{\Phi(A)}{\text{tr}(A)}\right) = \frac{\text{tr}(\Phi(A))}{\text{tr}(A)}$ donc $\text{tr}(\Phi(A)) = \text{tr}(A)$.

On peut alors prouver les deux points :

- i. $\forall A \in \mathcal{L}^+(\mathcal{H}_1)$ opérateur positif, on vient de montrer que $\Phi(A)$ est un opérateur positif.
- ii. Soit $A \in \mathcal{L}(\mathcal{H}_1)$.
 - Si A est un positif, on vient de montrer que $\text{tr}(\Phi(A)) = \text{tr}(A)$.
 - Sinon, on se ramène au cas positif en effectuant une décomposition autoadjoint-antiautoadjoint :

$$A = H + iK \quad \text{avec} \quad H = \frac{A + A^*}{2} \text{ et } K = \frac{A - A^*}{2} \text{ hermitiens}$$

(iK anti-hermitien). On effectue alors une décomposition en partie positive et négative⁸ de H :

$$\exists P_+, P_- \in \mathcal{L}^+(\mathcal{H}_1) : H = P_+ - P_-$$

et alors on a montré que $\text{tr}(\Phi(P_{\pm})) = \text{tr}(P_{\pm})$. Donc par linéarité de Φ et de la trace,

$$\text{tr}(\Phi(H)) = \text{tr}(\Phi(P_+ - P_-)) = \text{tr}(\Phi(P_+)) - \text{tr}(\Phi(P_-)) = \text{tr}(P_+) - \text{tr}(P_-) = \text{tr}(P_+ - P_-) = \text{tr}(H)$$

De même pour K hermitien : $\text{tr}(\Phi(K)) = \text{tr}(K)$. Donc, encore par linéarité,

$$\text{tr}(\Phi(A)) = \text{tr}(\Phi(H + iK)) = \text{tr}(\Phi(H)) + i \text{tr}(\Phi(K)) = \text{tr}(H) + i \text{tr}(K) = \text{tr}(H + iK) = \text{tr}(A)$$

□

Notons que l'on pourrait généraliser ce formalisme à des transformations de *trace non-croissante*, c'est-à-dire que $\forall P \in \mathcal{L}_{\text{tr } 1}^+(\mathcal{H}_1), \text{tr}(\Phi(P)) \leq 1$, sans se limiter aux transformations conservant la trace. C'est utile pour décrire les systèmes qui « fuient » dans leur environnement, par exemple des photons absorbés dans une fibre optique.

8. Si on a une matrice hermitienne $H \in \mathbb{M}_n(\mathbb{C})$, que l'on diagonalise en $H = O^{-1} \Delta O$ avec $\Delta = \text{diag}(\lambda_i)_i$, on pose

$$\begin{aligned} \Delta_+ &= \text{diag}(\lambda_i \mathbb{1}_{\lambda_i > 0})_i & \text{et} & & P_+ &= O^{-1} \Delta_+ O \in \mathbb{M}_n^+(\mathbb{C}) \text{ positive} \\ \Delta_- &= \text{diag}(-\lambda_i \mathbb{1}_{\lambda_i < 0})_i & \text{et} & & P_- &= O^{-1} \Delta_- O \in \mathbb{M}_n^+(\mathbb{C}) \text{ positive} \end{aligned}$$

et alors on a la décomposition $H = O^{-1}(\Delta_+ - \Delta_-)O = P_+ - P_-$.

1.3 Systèmes couplés et algèbre tensorielle

L'algèbre linéaire tensorielle est l'outil de choix pour décrire les systèmes quantiques couplés, par exemple deux particules, une particule et ses états internes, ou encore un système et son environnement, en particulier un système et un instrument de mesure. On verra par la suite qu'un canal quantique se comporte, par définition, de la bonne façon lorsqu'il est couplé avec un autre canal quantique. On présente donc assez rapidement les notions d'algèbre tensorielle qui nous serviront.

1.3.1 Produit tensoriel d'espaces vectoriels

Soient $\mathcal{V}, \mathcal{W}$ deux $\mathbb{K}$ -espaces vectoriels. Il existe un $\mathbb{K}$ -EV $\mathcal{V} \otimes \mathcal{W}$ et une application bilinéaire

$$\begin{aligned} \cdot \otimes \cdot &: \mathcal{V} \times \mathcal{W} \longrightarrow \mathcal{V} \otimes \mathcal{W} \\ v, w &\longmapsto v \otimes w \end{aligned}$$

qui vérifient une *propriété universelle* : toute application bilinéaire $f : \mathcal{V} \times \mathcal{W} \rightarrow \mathcal{Z}$ dans un $\mathbb{K}$ -EV $\mathcal{Z}$ se factorise de façon unique à travers $\varphi := \cdot \otimes \cdot$, c'est à dire que $\exists! \tilde{f} \in \mathcal{L}(\mathcal{V} \otimes \mathcal{W}, \mathcal{Z}) : f = \tilde{f} \circ \varphi$.

Autrement dit, pour tout $\mathbb{K}$ -EV $\mathcal{Z}$, on a une bijection

$$\begin{aligned} \mathcal{L}(\mathcal{V} \otimes \mathcal{W}, \mathcal{Z}) &\longleftrightarrow \mathcal{L}_2(\mathcal{V} \times \mathcal{W}, \mathcal{Z}) \\ f &\longmapsto ((v, w) \mapsto f(v \otimes w)) \end{aligned}$$

De plus, cet espace $\mathcal{V} \otimes \mathcal{W}$ est unique à isomorphisme de $\mathbb{K}$ -EV près, ce qui est clair grâce au fait que l'on demande une factorisation unique. On appelle $\mathcal{V} \otimes \mathcal{W}$ le **produit tensoriel** de $\mathcal{V}$ et $\mathcal{W}$. On trouvera une construction générale par quotient dans [Sage, §1.1] ou [Bertrand, §1.1]. On se restreint désormais à la dimension finie.

Donnons quelques propriétés importantes pour clarifier cette définition abstraite⁹ :

- $\forall v, v' \in \mathcal{V}, \forall w, w' \in \mathcal{W}, \quad (v + v') \otimes w = v \otimes w + v' \otimes w \quad \text{et} \quad v \otimes (w + w') = v \otimes w + v \otimes w'$
- $\forall \lambda \in \mathbb{K}, \forall v \in \mathcal{V}, \forall w \in \mathcal{W}, \quad \lambda \cdot (v \otimes w) = (\lambda \cdot v) \otimes w = v \otimes (\lambda \cdot w).$
- Si $(\hat{v}_i)_{1 \leq i \leq n}$ et $(\hat{w}_j)_{1 \leq j \leq m}$ sont des bases de $\mathcal{V}$ et $\mathcal{W}$ respectivement, alors [Sage, §1.2.2]
 $(\hat{v}_i \otimes \hat{w}_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ est une base de $\mathcal{V} \otimes \mathcal{W}$
- Ainsi, $\dim(\mathcal{V} \otimes \mathcal{W}) = \dim(\mathcal{V}) \times \dim(\mathcal{W})$ et $\mathcal{V} \otimes \mathcal{W} \cong \mathbb{K}^{nm}$. Mais on peut faire plus utile :
- $\forall x \in \mathcal{V} \otimes \mathcal{W}, \quad \exists! (v_j)_{1 \leq j \leq m} \in \mathcal{V}^m : x = \sum_{j=1}^m v_j \otimes \hat{w}_j$. Ainsi, $\mathcal{V} \otimes \mathcal{W} \cong \bigoplus^m \mathcal{V} \cong \mathcal{V}^{\dim \mathcal{W}}$, et on écrira $x \cong \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$ par cet isomorphisme. À noter que $\mathcal{V}^{\dim \mathcal{W}}$ n'est évidemment pas un $\mathcal{V}$ -espace vectoriel, et il faut voir ce vecteur comme un « vecteur par blocs » plus qu'un « vecteur de vecteurs », c'est pourquoi on préférera la notation $\bigoplus^m \mathcal{V}$, dans la continuité de l'idée de somme directe¹⁰. De même, $\mathcal{V} \otimes \mathcal{W} \cong \bigoplus^n \mathcal{W} \cong \mathcal{W}^{\dim \mathcal{V}}$.

Donnons une réalisation concrète du produit tensoriel d'espaces hilbertiens $(\mathcal{V}, \langle \cdot | \cdot \rangle_{\mathcal{V}})$ et $(\mathcal{W}, \langle \cdot | \cdot \rangle_{\mathcal{W}})$: $\forall v \in \mathcal{V}, w \in \mathcal{W}$, on peut définir $v \otimes w$ comme une forme bilinéaire $\mathcal{V} \times \mathcal{W} \rightarrow \mathbb{C}$ telle que :

$$\forall x \in \mathcal{V}, \forall y \in \mathcal{W}, \quad (v \otimes w)(x, y) = \langle v | x \rangle_{\mathcal{V}} \cdot \langle w | y \rangle_{\mathcal{W}}$$

En effet, cette construction vérifie la propriété universelle. On obtient du même coup que

$$\mathcal{V} \otimes \mathcal{W} \cong \mathcal{L}_2(\mathcal{V} \times \mathcal{W}, \mathbb{C}) \cong \mathbb{M}_{n,m}(\mathbb{C}) \cong \mathbb{C}^{nm} \quad (15)$$

9. Si l'intuition fait défaut : [The Tensor Product, Demystified](#)

10. La notation $\bigoplus^m V$ nécessiterai, si l'on voulait être tout à fait formel, de parler de l'espace dans lequel on fait la somme directe, alors que V^m est naturellement muni de la structure produit par les opérations composantes par composantes. La première notation est plus naturelle ici, la seconde plus rigoureuse a priori.

Écrivons ce troisième isomorphisme : $\forall v \in \mathcal{V}, \forall w \in \mathcal{W}$, si l'on décompose dans les bases de $\mathcal{V}$ et $\mathcal{W}$,

$$v \cong \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, w \cong \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix} \quad \text{et alors} \quad v \otimes w \cong \begin{bmatrix} \bar{v}_1 \bar{w}_1 & \cdots & \bar{v}_1 \bar{w}_m \\ \vdots & \ddots & \vdots \\ \bar{v}_n \bar{w}_1 & \cdots & \bar{v}_n \bar{w}_m \end{bmatrix}$$

Enfin, on peut naturellement munir $\mathcal{V} \otimes \mathcal{W}$ d'un produit scalaire hermitien, déterminé par :

$$\forall v_1, v_2 \in \mathcal{V}, \forall w_1, w_2 \in \mathcal{W}, \quad \langle v_1 \otimes w_1 | v_2 \otimes w_2 \rangle := \langle v_1 | v_2 \rangle_{\mathcal{V}} \cdot \langle w_1 | w_2 \rangle_{\mathcal{W}} \quad (16)$$

1.3.2 Produit tensoriel d'applications linéaire et produit de Kronecker

Soient $\varphi \in \mathcal{L}(\mathcal{X}, \mathcal{V})$ et $\psi \in \mathcal{L}(\mathcal{Y}, \mathcal{W})$ des applications linéaires entre espaces vectoriels. Alors on définit le **produit tensoriel** $\varphi \bar{\otimes} \psi : \mathcal{X} \otimes \mathcal{Y} \longrightarrow \mathcal{V} \otimes \mathcal{W}$ **des applications** φ **et** ψ , comme l'application linéaire déterminée par :

$$\forall x \in \mathcal{X}, \forall y \in \mathcal{Y}, \quad (\varphi \bar{\otimes} \psi)(x \otimes y) := \varphi(x) \otimes \psi(y)$$

Afin de mieux comprendre ce qu'est le produit tensoriel d'applications, cherchons d'abord à exprimer les endomorphismes $\mathcal{L}(\mathbb{K}^n \otimes \mathcal{V})$ sous forme matricielle. Si l'on note l'isomorphisme $\Xi : \mathbb{K}^n \otimes \mathcal{V} \cong \bigoplus^n \mathcal{V}$, et si l'on se donne une matrice d'opérateurs $\Phi = [\phi_{i,j}]_{1 \leq i, j \leq n} \in \mathbb{M}_n(\mathcal{L}(\mathcal{V}))$ (que l'on peut voir comme une matrice de $n \times n$ blocs), on peut construire un endomorphisme $\phi : \mathbb{K}^n \otimes \mathcal{V} \longrightarrow \mathbb{K}^n \otimes \mathcal{V}$ tel que

$$\forall x \in \mathbb{K}^n \otimes \mathcal{V}, \quad \Xi(\phi(x)) = \Phi \Xi(x) = \begin{bmatrix} \phi_{1,1} & \cdots & \phi_{1,n} \\ \vdots & \ddots & \vdots \\ \phi_{n,1} & \cdots & \phi_{n,n} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \in \bigoplus^n \mathcal{V} \quad \text{si} \quad [v_i]_{1 \leq i \leq n} = \Xi(x) \in \bigoplus^n \mathcal{V}$$

c'est à dire, plus explicitement, si l'on note $\mathcal{E} := (\hat{e}_i)_{1 \leq i \leq n}$ la base de $\mathbb{K}^n$,

$$\phi(x) = \Xi^{-1}(\Phi \Xi(x)) = \sum_{i=1}^n \hat{e}_i \otimes \sum_{j=1}^n \phi_{i,j}(v_j)$$

Réciproquement, soit $\phi \in \mathcal{L}(\mathbb{K}^n \otimes \mathcal{V})$, posons $\tilde{\phi} = \Xi \circ \phi \circ \Xi^{-1} \in \mathcal{L}\left(\bigoplus^n \mathcal{V}\right)$. Alors si l'on pose $\forall i, j \in \llbracket 1, n \rrbracket$

$$\begin{aligned} \phi_{i,j} \in \mathcal{L}(\mathcal{V}) \quad \text{tel que} \quad \forall v \in \mathcal{V}, \quad \phi_{i,j}(v) &= \pi_i \left(\tilde{\phi} \left([\mathbb{1}_{kj} \cdot v]_{1 \leq j \leq n} \right) \right) \\ &= \pi_i \left(\Xi(\phi(\hat{e}_j \otimes v)) \right) \end{aligned}$$

avec π_i la projection sur la i -ème sous-espace de $\bigoplus^n \mathcal{V}$, c'est-à-dire pour $j = 1$ par exemple,

$$\phi_{i,1}(v) = y_i \quad \text{lorsque} \quad \tilde{\phi} \begin{bmatrix} v \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$$

on retrouve la matrice d'opérateurs $\Phi = [\phi_{i,j}]_{1 \leq i, j \leq n} \in \mathbb{M}_n(\mathcal{L}(\mathcal{V}))$ associée. Ainsi, on a un isomorphisme

$$\mathcal{L}(\mathbb{K}^n \otimes \mathcal{V}) \cong \mathbb{M}_n(\mathcal{L}(\mathcal{V})) \quad (17)$$

Maintenant, si l'on se donne $\varphi \in \mathcal{L}(\mathbb{K}^n)$ et $\psi \in \mathcal{L}(\mathcal{V})$, alors $\phi := \varphi \bar{\otimes} \psi \in \mathcal{L}(\mathbb{K}^n \otimes \mathcal{V})$. On cherche à expliciter la matrice d'opérateurs associée à $\varphi \bar{\otimes} \psi$. Posons

$$A = [a_{ij}]_{1 \leq i, j \leq n} := \text{mat}_{\mathcal{E}}(\varphi)$$

Alors $\forall v \in \mathcal{V}, \forall j \in \llbracket 1, n \rrbracket$,

$$(\varphi \bar{\otimes} \psi)(\hat{e}_j \otimes v) = \varphi(\hat{e}_j) \otimes \psi(v) = \left(\sum_{k=1}^n a_{kj} \hat{e}_k \right) \otimes \psi(v) = \sum_{k=1}^n \hat{e}_k \otimes (a_{kj} \psi(v))$$

$$\text{donc} \quad \Xi((\varphi \bar{\otimes} \psi)(\hat{e}_j \otimes v)) = [a_{kj} \psi(v)]_{1 \leq k \leq n}$$

$$\text{donc } \forall i, j \in \llbracket 1, n \rrbracket, \quad \phi_{ij}(v) = \pi_i(\Xi(\phi(\hat{e}_j \otimes v))) = \pi_i([a_{kj} \psi(v)]_{1 \leq k \leq n}) = a_{ij} \psi(v)$$

Ainsi, la matrice d'opérateurs associée par l'isomorphisme (17) à $\varphi \bar{\otimes} \psi$ est

$$[\phi_{ij}]_{1 \leq i, j \leq n} = [a_{ij} \psi]_{1 \leq i, j \leq n} = \begin{bmatrix} a_{11} \psi & \cdots & a_{1n} \psi \\ \vdots & \ddots & \vdots \\ a_{n1} \psi & \cdots & a_{nn} \psi \end{bmatrix} \in \mathbb{M}_n(\mathcal{L}(\mathcal{V})) \quad (18)$$

Par exemple pour $n = 2$ et $B = \text{mat}(\psi) = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, on peut associer à $\varphi \bar{\otimes} \psi$ la matrice par blocs

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \bar{\otimes} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} := \begin{bmatrix} a_{11} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}$$

que l'on appelle le **produit de Kronecker** des deux matrices A et B , et que l'on note $A \bar{\otimes} B$. Dans toute la suite, on identifie $\mathbb{M}_n(\mathbb{M}_m(\mathbb{C})) = \mathbb{M}_{(nm)}(\mathbb{C})$. On remarque que l'on peut écrire, de façon unique,

$$A \bar{\otimes} B = \hat{E}_{11} \bar{\otimes} C_{11} + \hat{E}_{12} \bar{\otimes} C_{12} + \hat{E}_{21} \bar{\otimes} C_{21} + \hat{E}_{22} \bar{\otimes} C_{22}$$

avec $(\hat{E}_{ij})_{1 \leq i, j \leq 2}$ base canonique de $\mathbb{M}_2(\mathbb{K})$, et $C_{ij} = a_{ij}B$.

On remarque alors que le résultat (18) se reformule de façon similaire : si on pose $(\hat{e}_{ij})_{1 \leq i, j \leq n}$ la base canonique de $\mathcal{L}(\mathbb{K}^n)$ (c'est-à-dire $\text{mat}_{\mathcal{E}}(\hat{e}_{ij}) = E_{ij}$), on a :

$$\phi = \varphi \bar{\otimes} \psi = \sum_{1 \leq i, j \leq n} \hat{e}_{ij} \bar{\otimes} \phi_{ij} \quad \text{avec} \quad [\phi_{ij}]_{1 \leq i, j \leq n} \stackrel{\text{rappel}}{=} \text{mat}_{\mathcal{E}}(\varphi) \cdot \psi \quad (19)$$

c'est à dire que $\mathcal{L}(\mathbb{K}^n \otimes \mathcal{V}) \cong \bigoplus^{n \times n} \mathcal{L}(\mathcal{V}) \cong \mathbb{M}_n(\mathcal{L}(\mathcal{V}))$. Alors grâce à l'isomorphisme $\bigoplus^{n \times n} \mathcal{L}(\mathcal{V}) \cong \mathcal{L}(\mathbb{K}^n) \otimes \mathcal{L}(\mathcal{V})$, on peut finalement écrire :

$$\phi \cong \sum_{1 \leq i, j \leq n} \hat{e}_{ij} \otimes \phi_{ij} \in \mathcal{L}(\mathbb{K}^n) \otimes \mathcal{L}(\mathcal{V})$$

Et puisque $(\hat{e}_{ij})_{1 \leq i, j \leq n}$ est une base, ces objets engendrent $\mathcal{L}(\mathbb{K}^n) \otimes \mathcal{L}(\mathcal{V})$ et on a un isomorphisme

$$\begin{aligned} \mathcal{L}(\mathbb{K}^n) \otimes \mathcal{L}(\mathcal{V}) &\xleftarrow{\cong} \mathbb{M}_n(\mathcal{L}(\mathcal{V})) \xleftarrow{\cong} \mathcal{L}(\mathbb{K}^n \otimes \mathcal{V}) \\ \sum_{1 \leq i, j \leq n} \hat{e}_{ij} \otimes \phi_{ij} &\longmapsto [\phi_{ij}]_{1 \leq i, j \leq n} \longmapsto \sum_{1 \leq i, j \leq n} \hat{e}_{ij} \bar{\otimes} \phi_{ij} \end{aligned} \quad (20)$$

Noter la subtile différence : à droite, on a un produit tensoriel d'applications ($\bar{\otimes}$), ce qui donne une *application* dans $\mathbb{K}^n \otimes \mathcal{V}$, alors qu'à gauche, on voit cette application comme un *vecteur* de l'espace tensoriel $\mathcal{L}(\mathbb{K}^n) \otimes \mathcal{L}(\mathcal{V})$, décomposé tensoriellement ($\otimes$) dans la base $(\hat{e}_{ij})_{1 \leq i, j \leq n}$ de $\mathcal{L}(\mathbb{K}^n)$.

En particulier, $\forall \phi \in \mathcal{L}(\mathbb{K}^n \otimes \mathcal{V})$,

$$\exists ! [\phi_{ij}]_{1 \leq i, j \leq n} \in \mathbb{M}_n(\mathcal{L}(\mathcal{V})) : \phi = \sum_{1 \leq i, j \leq n} \hat{e}_{ij} \bar{\otimes} \phi_{ij} \quad (21)$$

De façon similaire, sous forme purement matricielle (c'est-à-dire pour le produit de Kronecker),

$$\mathbb{M}_n(\mathbb{K}) \otimes \mathbb{M}_m(\mathbb{K}) \cong \mathbb{M}_{n \cdot m}(\mathbb{K}) \cong \mathcal{L}(\mathbb{K}^n \otimes \mathbb{K}^m) \hookleftarrow \mathbb{M}_n(\mathbb{K}) \bar{\otimes} \mathbb{M}_m(\mathbb{K}) \quad (22)$$

Cet isomorphisme nous permet, dans la suite, de noter $\otimes$ à la place de $\bar{\otimes}$. Il se généralise bien sûr en

$$\mathcal{L}(\mathcal{V}) \otimes \mathcal{L}(\mathcal{W}) \cong \mathcal{L}(\mathcal{V} \otimes \mathcal{W})$$

qu'on appelle le **morphisme de Kronecker**.

Donnons enfin une caractérisation de la positivité pour les opérateurs hermitiens de $\mathcal{V} \otimes \mathbb{C}^n$.

Soit $\phi \in \mathcal{L}(\mathcal{V} \otimes \mathbb{C}^n)$ et $x \in \mathcal{V} \otimes \mathbb{C}^n$, que l'on peut écrire $x = \sum_{i=1}^n v_i \otimes \hat{e}_i$ avec $[v_i]_{1 \leq i \leq n} = \Xi(x)$. Alors

$$\begin{aligned}
\langle x, \phi(x) \rangle &= \left\langle x, \left(\sum_{k,l} \phi_{kl} \bar{\otimes} \hat{e}_{kl} \right) \left(\sum_i v_i \otimes \hat{e}_i \right) \right\rangle \\
[\text{linéarité de } \phi] &= \left\langle x, \sum_i \left(\sum_{k,l} \phi_{kl} \bar{\otimes} \hat{e}_{kl} \right) (v_i \otimes \hat{e}_i) \right\rangle \\
[\text{définition du produit } \bar{\otimes}] &= \left\langle x, \sum_i \sum_{k,l} \phi_{kl} (v_i \otimes \hat{e}_{kl}(\hat{e}_i)) \right\rangle \\
[\hat{e}_{kl}(\hat{e}_i) = \mathbb{1}_{ki} \hat{e}_l] &= \left\langle \sum_j v_j \otimes \hat{e}_j, \sum_i \sum_l \phi_{il} (v_i \otimes \hat{e}_l) \right\rangle \\
[\text{linéarité de } \langle \cdot, \cdot \rangle] &= \sum_{i,j,l} \langle v_j \otimes \hat{e}_j, \phi_{il} (v_i \otimes \hat{e}_l) \rangle \\
[\text{définition (16) de } \langle \cdot, \cdot \rangle_{\mathcal{V} \otimes \mathbb{C}^n}] &= \sum_{i,j,l} \langle v_j, \phi_{il} (v_i) \rangle \cdot \langle \hat{e}_j, \hat{e}_l \rangle \\
[\langle \hat{e}_j, \hat{e}_l \rangle = \mathbb{1}_{jl}] &= \sum_{i,j} \langle v_j, \phi_{ij} (v_i) \rangle
\end{aligned}$$

En parallèle, lorsqu'on considère la matrice associée à l'opérateur, on retrouve

$$\begin{aligned}
\left\langle \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, \begin{bmatrix} \phi_{1,1} & \cdots & \phi_{1,n} \\ \vdots & \ddots & \vdots \\ \phi_{n,1} & \cdots & \phi_{n,n} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \right\rangle &= \left\langle \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, \begin{bmatrix} \sum_j \phi_{1,j}(v_j) \\ \vdots \\ \sum_j \phi_{n,j}(v_j) \end{bmatrix} \right\rangle = \sum_j \left\langle \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, \begin{bmatrix} \phi_{1,j}(v_j) \\ \vdots \\ \phi_{n,j}(v_j) \end{bmatrix} \right\rangle \\
&= \sum_{i,j} \langle v_j, \phi_{ij}(v_i) \rangle = \langle x, \phi(x) \rangle
\end{aligned}$$

Ainsi, pour vérifier la positivité d'un opérateur sur $\mathcal{V} \otimes \mathbb{C}^n$, il suffit de la vérifier sur la matrice associée :

Proposition 2. Soit $\phi \in \mathcal{L}(\mathcal{V} \otimes \mathbb{C}^n)$. Si l'on considère la décomposition de ϕ dans $(\hat{e}_{ij})_{1 \leq i,j \leq n}$, on a

$$\begin{aligned}
\phi = \sum_{i,j} \phi_{ij} \bar{\otimes} \hat{e}_{ij} \in \mathcal{L}^+(\mathcal{V} \otimes \mathbb{C}^n) \text{ positif} &\iff \forall (v_i)_{1 \leq i \leq n} \in \mathcal{V}^n, \quad \sum_{i,j} \langle v_j, \phi_{ij}(v_i) \rangle \geq 0 \\
&\iff [\phi_{ij}]_{1 \leq i,j \leq n} \text{ positive}
\end{aligned}$$

1.3.3 Couplage de système quantiques

On utilise maintenant le produit tensoriel pour décrire l'espace des états d'un couplage de systèmes quantiques, et le produit tensoriel d'applications pour décrire l'évolution de ce système couplé :

Axiome 5. Considérons deux systèmes représentés par les espaces des états $\mathcal{H}_1$ et $\mathcal{H}_2$. Alors lorsque les deux systèmes sont couplés, l'espace des états du système total est le produit tensoriel $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Deux systèmes sont couplés par exemple pendant ou après une interaction. Si le système 1 se trouve (par exemple avant une interaction) dans l'état pur $\psi_1 \in \mathcal{H}_1$ et le système 2 dans l'état pur $\psi_2 \in \mathcal{H}_2$, alors le système total est dans l'état $\psi_1 \otimes \psi_2$: on dit que l'état du système total est *factorisé*. Mais, bien évidemment, les états du système couplé ne sont pas, en général, factorisés sous forme $\psi_1 \otimes \psi_2$ avec $\psi_1 \in \mathcal{H}_1$ et $\psi_2 \in \mathcal{H}_2$. On est alors en présence d'un état dit **intriqué**. Même très longtemps (et très loin) après une interaction, le système total peut rester intriqué.

En théorie quantique de l'information, cette notion est utilisée pour décrire le couplage d'un système avec son environnement (décohérence d'un qubit, interaction atome-champ...), avec un appareil de mesure (théorie de la mesure quantique), ou avec un autre système identique avec lequel il est intriqué (statistiques de Bell, téléportation quantique, cryptographie quantique...).

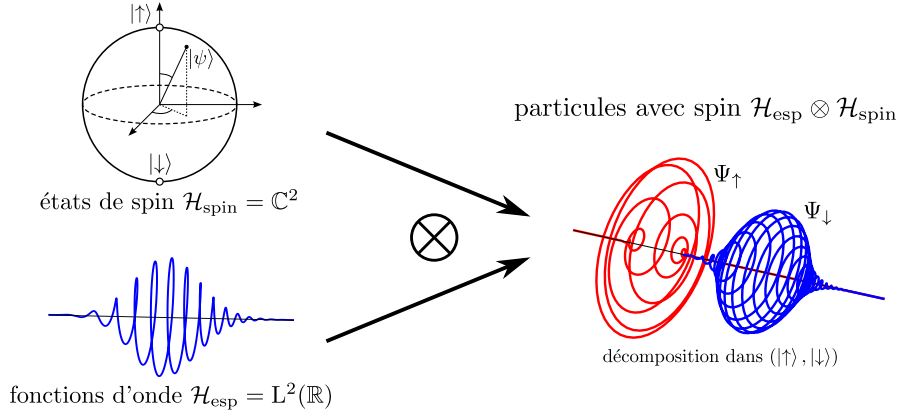


FIGURE 5 – En physique, cette notion de couplage est par exemple utilisée pour décrire une particule, $\mathcal{H}_{\text{esp}} = L^2(\mathbb{R}^d)$, possédant un *degré de liberté interne*, par exemple un spin $1/2$, $\mathcal{H}_{\text{spin}} = \text{Vect}(|\uparrow\rangle, |\downarrow\rangle) \cong \mathbb{C}^2$ (notation de Dirac), comme le produit tensoriel $\mathcal{H} = \mathcal{H}_{\text{esp}} \otimes \mathcal{H}_{\text{spin}}$. Un état peut alors s'écrire $|\Psi\rangle = |\Psi_{\uparrow}\rangle \otimes |\uparrow\rangle + |\Psi_{\downarrow}\rangle \otimes |\downarrow\rangle$ (par l'isomorphisme $\mathcal{H}_{\text{esp}} \otimes \mathcal{H}_{\text{spin}} \cong L^2 \oplus L^2$), et l'on dit que $|\Psi_{\uparrow}\rangle \in \mathcal{H}_{\text{esp}}$ est la composante de spin up de la fonction d'onde, et $|\Psi_{\downarrow}\rangle \in \mathcal{H}_{\text{esp}}$ celle de spin down. Elles vérifient $\int (|\Psi_{\uparrow}|^2 + |\Psi_{\downarrow}|^2) = 1$.

Axiome 6. *Considérons une évolution du système quantique 1, représentée par l'opérateur d'évolution*

$$\Phi_1 : \mathcal{L}(\mathcal{H}_1) \longrightarrow \mathcal{L}(\mathcal{H}_{o,1})$$

et, une évolution du système quantique 2, représentée par l'opérateur d'évolution

$$\Phi_2 : \mathcal{L}(\mathcal{H}_2) \longrightarrow \mathcal{L}(\mathcal{H}_{o,2})$$

(on les considère ici indépendamment l'une de l'autre, par exemple deux systèmes isolés). Alors, lorsque l'on regarde le système total $\mathcal{H}_1 \otimes \mathcal{H}_2$, l'évolution combinée du système total est représentée par

$$\Phi_1 \otimes \Phi_2 : \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2) \longrightarrow \mathcal{L}(\mathcal{H}_{o,1} \otimes \mathcal{H}_{o,2})$$

Bien sûr, lorsque l'évolution d'un système dépend de l'état de l'autre, on ne peut pas parler de l'évolution d'un système ou de l'autre (c'est-à-dire de Φ_1 ou Φ_2). L'évolution est alors plus complexe, mais reste souvent exprimée grâce à des produits tensoriels d'applications¹¹.

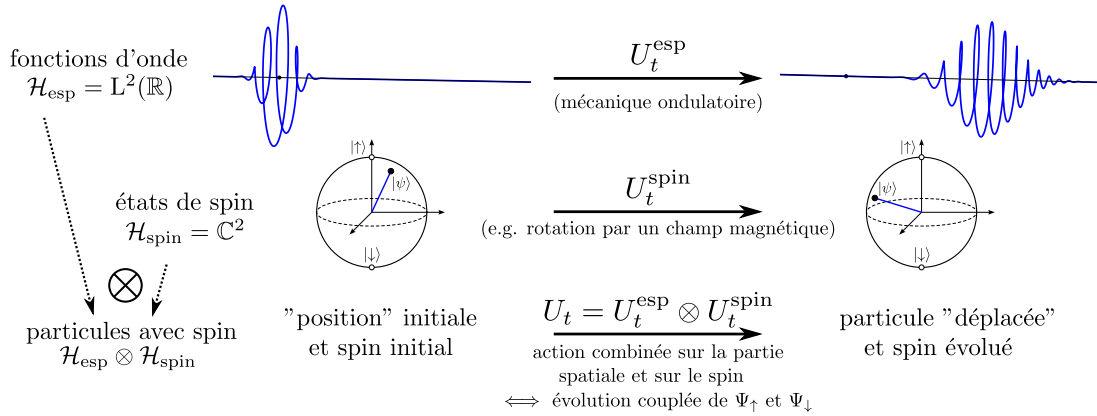


FIGURE 6 – Illustration de l'évolution de l'exemple précédent de la particule avec spin, comme couplage de l'évolution qu'aurait une particule simple se « déplaçant » d'une part, et de l'évolution qu'aurait un spin $1/2$ abstrait d'autre part. Pour obtenir une telle évolution, il faut que l'évolution de la fonction d'onde soit indépendante du spin, et que l'évolution du spin soit indépendante de la « position » de la particule (c'est le cas quand le champ magnétique est homogène par exemple).

11. Dans le cas simple où les deux systèmes sont indépendants et ont une évolution hamiltonienne, on peut chercher à donner l'hamiltonien du système total : si l'on a $i\hbar \partial_t U_{1,t} = H_1(t)U_{1,t}$ et $i\hbar \partial_t U_{2,t} = H_2(t)U_{2,t}$, alors en admettant la formule de Leibniz pour le produit tensoriel (se voit aisément avec la produit de Kronecker), on a

$$\begin{aligned} HU_t &\stackrel{\text{Schrö.}}{=} i\hbar \partial_t U_t \stackrel{\text{axiome}}{=} i\hbar \partial_t (U_{1,t} \otimes U_{2,t}) \stackrel{\text{Leibniz}}{=} i\hbar (\partial_t U_{1,t} \otimes U_{2,t}) + i\hbar (U_{1,t} \otimes \partial_t U_{2,t}) \\ &\stackrel{\text{Schrö.}}{=} H_1 U_{1,t} \otimes U_{2,t} + U_{1,t} \otimes H_2 U_{2,t} \stackrel{\text{def}}{=} (H_1 \otimes \mathbb{1}_2)(U_{1,t} \otimes U_{2,t}) + (\mathbb{1}_1 \otimes H_2)(U_{1,t} \otimes U_{2,t}) \end{aligned}$$

donc $H(t) = H_1(t) \otimes \mathbb{1}_2 + \mathbb{1}_1 \otimes H_2(t)$.

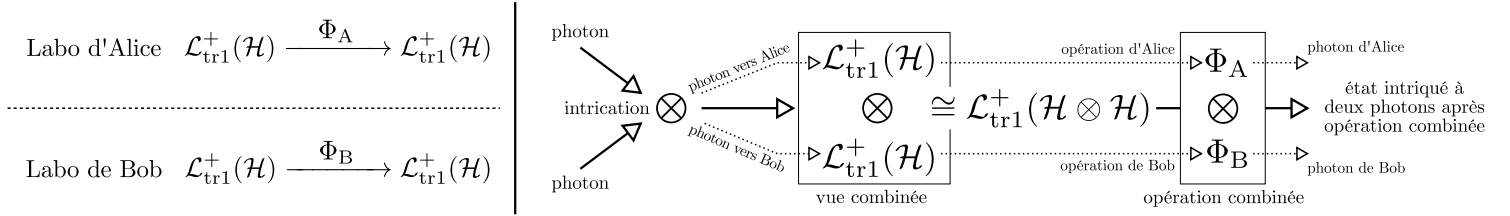


FIGURE 7 – Illustration du couplage de deux photons ($\mathcal{H} = \mathcal{H}_{\text{photon}}$) et de leur évolution. à gauche, situation des deux laboratoires manipulant un photon avec Φ_A et Φ_B . à droite, exemple où il est nécessaire de voir les deux laboratoires de façon combinée : on prépare deux photons intriqués (état P non factorisé) et on envoie chaque « photon » vers Alice et Bob. Chacun effectue une opération sur son photon, indépendamment de l'autre laboratoire, mais si l'on veut par exemple expliquer les éventuelles corrélations entre les mesures d'Alice et de Bob, il faut considérer $(\Phi_A \otimes \Phi_B)(P)$.

2 Canaux quantiques, complète positivité et théorème de Choi-Kraus

La question naturelle qui se pose maintenant est la suivante : $\Phi_1 \otimes \Phi_2$ est-il un opérateur d'évolution ? Dit autrement, les mélanges d'états de $\mathcal{H}_1 \otimes \mathcal{H}_2$ sont-ils encore envoyés sur des opérateurs statistiques de $\mathcal{H}_{o,1} \otimes \mathcal{H}_{o,2}$?

La réponse est négative en général : comme on le verra dans le contre-exemple 5, on peut construire une transformation positive Φ telle que $\Phi \otimes \text{id}_{\mathcal{L}(\mathbb{C}^2)}$ ne préserve pas la positivité.

Ainsi, si l'on veut que les opérateurs statistiques soient les descriptions les plus générales d'un système quantique lorsque l'on considère les systèmes couplés, il est nécessaire d'imposer une condition aux opérateurs d'évolution dans le postulat 4. On appelle de telles transformations des *canaux quantiques*.

2.1 Canaux quantiques

Axiome 7. *Les canaux quantiques sont des opérateurs d'évolution (c'est-à-dire des transformations linéaires envoyant les opérateurs statistiques sur des opérateurs statistiques) telles que le couplage (c'est-à-dire le produit tensoriel) de deux canaux quantiques est encore un opérateur d'évolution. On impose à l'identité d'être un canal quantique.*

En l'état, cette définition n'est pas bien définie mathématiquement, et c'est justement le but de ce document que de donner une définition « équivalente » précise de ce qu'est un canal quantique. On rappelle qu'il est équivalent de demander aux opérateurs d'évolution d'être des transformations positives et préservant la trace, par le théorème 1.

Les canaux quantiques modélisent bien évidemment les canaux de communication quantique, mais c'est une notion bien plus générale : un *instrument quantique* est par exemple décrit comme un cas particulier de « canal » quantique, dont l'espace des résultats $\mathcal{H}_o = \mathcal{H}_2 \otimes \mathbb{C}^{\text{Issues}}$ est formé de l'espace où vit l'état après mesure ainsi que de l'espace décrivant l'état de l'instrument, classique, après la mesure.

2.2 Complète positivité

Pour introduire la notion d'application complètement positive, considérons deux canaux :

- le premier quelconque, avec $\Phi = \Phi_1 : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H})$ transformation positive préservant la trace
- le deuxième trivial, avec $\Phi_2 = \text{id}_{\mathcal{L}(\mathbb{C}^n)} =: \text{id}_n$ (c'est à dire n'agissant pas sur le système quantique)

avec $n \in \mathbb{N}^*$. Alors l'axiome des canaux quantiques impose à

$$\Phi_1 \otimes \Phi_2 = \Phi \otimes \text{id}_n : \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^n) \rightarrow \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^n)$$

d'être une transformation positive et préservant la trace. Et ceci pour tout $n \in \mathbb{N}^*$.

Définition 3. Une transformation linéaire $\Phi : \mathcal{L}(\mathcal{H}_1) \longrightarrow \mathcal{L}(\mathcal{H}_2)$ est dite **n -positive** si $\Phi \otimes \text{id}_n$ est positive. Cette transformation est dite **complètement positive** si $\forall n \in \mathbb{N}^*$, Φ est n -positive.

Une transformation est positive si et seulement si elle est 1-positive. L'exemple précédent impose à tout canal quantique d'être complètement positif.

Donnons tout d'abord une caractérisation matricielle, plus pratique, de la n -positivité. Soit un opérateur $\mathbf{A} \in \mathcal{L}(\mathcal{H}_1 \otimes \mathbb{C}^n)$. Par l'isomorphisme $\mathcal{L}(\mathcal{H}_1 \otimes \mathbb{C}^n) \cong \mathcal{L}(\mathcal{H}_1) \otimes \mathcal{L}(\mathbb{C}^n) \cong \mathbb{M}_n(\mathcal{L}(\mathcal{H}_1))$ (20) avec la base canonique $(E_{ij})_{1 \leq i, j \leq n}$ de $\mathcal{L}(\mathbb{C}^n)$, on écrit $\mathbf{A} = \sum_{1 \leq i, j \leq n} A_{ij} \otimes E_{ij} \cong [A_{ij}]_{1 \leq i, j \leq n}$ puis

$$(\Phi \otimes \text{id}_n)(\mathbf{A}) = (\Phi \otimes \text{id}_n) \left(\sum_{i, j} A_{ij} \otimes E_{ij} \right) = \sum_{i, j} (\Phi \otimes \text{id}_n)(A_{ij} \otimes E_{ij}) = \sum_{i, j} \Phi(A_{ij}) \otimes \overbrace{\text{id}_n(E_{ij})}^{= E_{ij}}$$

par définition du produit tensoriel d'applications. De nouveau à travers l'isomorphisme $\mathcal{L}(\mathcal{H}_2 \otimes \mathbb{C}^n) \cong \mathbb{M}_n(\mathcal{L}(\mathcal{H}_2))$, on identifie $(\Phi \otimes \text{id}_n)(\mathbf{A})$ à la matrice d'opérateurs $[\Phi(A_{ij})]_{1 \leq i, j \leq n}$, donc $\Phi \otimes \text{id}_n$ à

$$\begin{aligned} \Phi^{[n]} : \mathbb{M}_n(\mathcal{L}(\mathcal{H}_1)) &\longrightarrow \mathbb{M}_n(\mathcal{L}(\mathcal{H}_2)) \\ [A_{ij}]_{i, j} &\longmapsto [\Phi(A_{ij})]_{i, j} \end{aligned} \quad (23)$$

Maintenant, en appliquant la proposition 2 deux fois, pour $\mathcal{L}^+(\mathcal{H}_1 \otimes \mathbb{C}^n)$ et $\mathcal{L}^+(\mathcal{H}_2 \otimes \mathbb{C}^n)$,

$$\begin{aligned} \Phi \otimes \text{id}_n \text{ transformation positive} &\iff \forall \mathbf{A} \in \mathcal{L}^+(\mathcal{H}_1 \otimes \mathbb{C}^n), (\Phi \otimes \text{id}_n)(\mathbf{A}) \in \mathcal{L}^+(\mathcal{H}_2 \otimes \mathbb{C}^n) \\ [\text{prop. 2}] &\iff \forall [A_{ij}]_{i, j} \text{ positive}, [\Phi(A_{ij})]_{i, j} \text{ positive} \\ &\iff \Phi^{[n]} \text{ transformation positive} \end{aligned}$$

c'est à dire si l'application associée $\Phi^{[n]}$ envoie les matrices positives sur des matrices positives. Ainsi,

Proposition 4. Soit $\Phi : \mathcal{L}(\mathcal{H}_1) \longrightarrow \mathcal{L}(\mathcal{H}_2)$ une transformation linéaire.

$$\Phi \text{ est complètement positive} \iff \forall n \in \mathbb{N}^*, \quad \Phi^{[n]} \text{ est positive}$$

On peut maintenant exhiber un contre exemple de complète positivité :

Exemple 5. Considérons l'application de transposition :

$$\begin{aligned} \Phi : \mathbb{M}_n(\mathbb{C}) &\longrightarrow \mathbb{M}_n(\mathbb{C}) \\ A &\longmapsto {}^t A \end{aligned}$$

C'est une transformation positive : $\forall A \in \mathbb{M}_n^+(\mathbb{C})$ positive, $\exists W \in \mathbb{M}_n(\mathbb{C}) : A = W^2$, donc $\Phi(A) = {}^t A = {}^t(W^2) = ({}^t W)^2 \in \mathbb{M}_n^+(\mathbb{C})$ est encore positive.

Par contre, elle n'est pas 2-positive car $\Phi^{[2]}$ elle ne conserve pas la positivité :

- $E = \begin{bmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{bmatrix}$ est une matrice positive (avec $(E_{ij})_{1 \leq i, j \leq n}$ la base canonique de $\mathbb{M}_n(\mathbb{C})$), car dans la base canonique $(e_i)_{1 \leq i \leq n}$ de $\mathbb{C}^n$, on a $\forall X = [x_i]_i, Y = [y_i]_i$,

$$\begin{aligned} \left\langle \begin{bmatrix} X \\ Y \end{bmatrix}, \begin{bmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \right\rangle &= \langle X, E_{11}X \rangle + \langle X, E_{12}Y \rangle + \langle Y, E_{21}X \rangle + \langle Y, E_{22}Y \rangle \\ &= \bar{x}_1 x_1 + \bar{x}_1 y_2 + \bar{y}_2 x_1 + \bar{y}_2 y_2 = |x_1 + y_2|^2 \geq 0 \end{aligned}$$

- Mais $\Phi^{[2]}(E) = \begin{bmatrix} {}^t E_{11} & {}^t E_{12} \\ {}^t E_{21} & {}^t E_{22} \end{bmatrix} = \begin{bmatrix} E_{11} & E_{21} \\ E_{12} & E_{22} \end{bmatrix}$ n'est pas une matrice positive car -1 est une valeur propre négative : puisque car $E_{ij} e_k = \mathbb{1}_{kj} e_i$, on a $\begin{bmatrix} E_{11} & E_{21} \\ E_{12} & E_{22} \end{bmatrix} \begin{bmatrix} e_2 \\ -e_1 \end{bmatrix} = \begin{bmatrix} 0 - e_2 \\ e_1 + 0 \end{bmatrix} = - \begin{bmatrix} e_2 \\ -e_1 \end{bmatrix}$.

2.3 Représentation de Choi-Kraus

En guise d'échauffement, commençons par un résultat simple :

Proposition 6. *L'évolution (14)*

$$\Phi_m : A \mapsto \sum_{k=1}^m M_k A M_k^*$$

associée au système de mesure $(M_k : \mathcal{H}_s \rightarrow \mathcal{H}_o)_{1 \leq k \leq m}$ est une transformation complètement positive.

Démonstration. Montrons-le en deux étapes :

1. D'abord, si $M \in \mathcal{L}(\mathcal{H}_s, \mathcal{H}_o)$, la transformation $\Phi_M : A \mapsto M A M^*$ est complètement positive par la proposition (4) puisque $\forall n \in \mathbb{N}^*$,

$$\Phi_M^{[n]} : [A_{ij}]_{i,j} \mapsto [\Phi(A_{ij})]_{i,j} = [M A_{ij} M^*]_{i,j}$$

est une transformation positive : $\forall \mathbf{A} = [A_{ij}]_{i,j} \in \mathbb{M}_n(\mathcal{L}(\mathcal{H}_s))$ positive, $\Phi_M^{[n]}(\mathbf{A})$ est positive car

$$\begin{aligned} \forall \chi = (\chi_i)_{1 \leq i \leq n} \in \mathcal{H}_o^n, \quad \langle \chi \mid \Phi_M^{[n]}(\mathbf{A}) \cdot \chi \rangle &= \left\langle \begin{bmatrix} \chi_1 \\ \vdots \\ \chi_n \end{bmatrix}, \begin{bmatrix} M A_{11} M^* & \cdots & M A_{1n} M^* \\ \vdots & \ddots & \vdots \\ M A_{n1} M^* & \cdots & M A_{nn} M^* \end{bmatrix} \begin{bmatrix} \chi_1 \\ \vdots \\ \chi_n \end{bmatrix} \right\rangle \\ [\text{car } \langle \chi \mid M A M^* \chi \rangle = \langle (M^* \chi) \mid A (M^* \chi) \rangle] &= \left\langle \begin{bmatrix} M^* \chi_1 \\ \vdots \\ M^* \chi_n \end{bmatrix}, \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix} \begin{bmatrix} M^* \chi_1 \\ \vdots \\ M^* \chi_n \end{bmatrix} \right\rangle \\ [\text{positivité de } \mathbf{A}] &= \langle \chi' \mid \mathbf{A} \cdot \chi' \rangle \geq 0 \end{aligned}$$

2. Maintenant, la transformation Φ_m est complètement positive car $\forall n \in \mathbb{N}^*$,

$$\Phi_m \otimes \text{id}_n = \sum_{k=1}^m \underbrace{(A \mapsto M_k A M_k^*)}_{\text{transformation positive}} \otimes \text{id}_n \text{ est une transformation positive}$$

simplement comme somme de transformation positive (par le premier point). En effet, si on l'évalue en une matrice positive $\mathbf{A} \in \mathbb{M}_n(\mathcal{L}(\mathcal{H}_s))$, on obtient une somme de matrices positives, donc encore une matrice positive (par linéarité du produit scalaire). □

Voici enfin le théorème central de cette discussion :

Théorème 7 (Choi [1975]). *Soit $\Phi : \mathbb{M}_n(\mathbb{C}) \rightarrow \mathbb{M}_m(\mathbb{C})$ une transformation linéaire.*

On a équivalence entre les propositions suivantes :

- a) Φ est complètement positive
- b) Φ est n -positive
- c) La **matrice de Choi** $\mathbf{C}_\Phi := [\Phi(E_{ij})]_{1 \leq i,j \leq n} = \Phi^{[n]}([E_{ij}]_{i,j}) \in \mathbb{M}_{(nm)}(\mathbb{C})$ est positive
- d) $\exists r \in \mathbb{N}, \exists (W_k)_{1 \leq k \leq r} \in \mathbb{M}_{m,n}(\mathbb{C})^r : \Phi = A \mapsto \sum_{k=1}^r W_k A W_k^*$.
On appelle de tels $(W_k)_{1 \leq k \leq r}$ des **opérateurs de Kraus**.

*Si on appelle le **rang de Choi**, noté $\text{cr}(\Phi)$, le nombre r minimal d'opérateurs de Kraus permettant une telle décomposition, on a alors $\text{cr}(\Phi) = \text{rang}(\mathbf{C}_\Phi)$.*

Remarque. On préfère ici le formalisme matriciel pour faciliter la démonstration, mais le résultat est évidemment toujours vrai avec $\Phi : \mathcal{L}(\mathcal{H}_1) \rightarrow \mathcal{L}(\mathcal{H}_2)$ et avec les $W_k \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$.

Démonstration. On abrège ici $\mathbb{M}_{p,q}(\mathbb{C})$ par $\mathbb{M}_{p,q}$.

(a $\Rightarrow$ b) : Par définition, une transformation complètement positive est en particulier n -positive.

(b $\Rightarrow$ c) : On rappelle que les matrices $E_{ij} = [\mathbb{1}_{ki} \mathbb{1}_{lj}]_{1 \leq i, j \leq n}$ vérifient $E_{ij}^* = E_{ji}$ et $E_{ij} E_{kl} = \mathbb{1}_{jk} E_{il}$.

Posons le produit tensoriel (que l'on peut aussi voir comme une somme de produits de Kronecker)

$$E := [E_{ij}]_{1 \leq i, j \leq n} \cong \sum_{1 \leq i, j \leq n} E_{ij} \otimes E_{ij}$$

(par $\mathbb{M}_n \otimes \mathbb{M}_n \cong \mathbb{M}_{n^2}$). On vérifie que, par transposition et produit par blocs,

$$E^* = [E_{ij}]_{i,j}^* = [E_{ji}^*]_{i,j} = [E_{ij}]_{i,j} = E$$

$$E^2 = [\sum_{k=1}^n E_{ik} E_{kj}]_{i,j} = [\sum_{k=1}^n E_{ij}]_{i,j} = [n E_{ij}]_{i,j} = n E$$

donc $E = \frac{1}{n} E E^*$, donc E est une matrice positive. On peut aussi voir que les seules valeurs propres possibles vérifient $\lambda^2 = n\lambda$, donc $\lambda \in \{0, n\}$, donc sont positives.

Maintenant, puisque Φ est n -positive, $\Phi^{[n]}$ est une transformation positive par une proposition précédente, donc la matrice de Choi $C_\Phi = \Phi^{[n]}(E)$ est une matrice positive. On peut aussi dire que comme $\Phi \otimes \text{id}_n$ est une transformation positive par définition et que $\sum_{i,j} E_{ij} \otimes E_{ij}$ est positive, alors

$$(\Phi \otimes \text{id}_n) \left(\sum_{i,j} E_{ij} \otimes E_{ij} \right) = \sum_{i,j} \Phi(E_{ij}) \otimes E_{ij} \cong [\Phi(E_{ij})]_{i,j} \text{ est positive}$$

(c $\Rightarrow$ d) ¹² : Puisque $C_\Phi \in \mathbb{M}_{(nm)}$ est positive, sa décomposition spectrale nous donne des couples vecteurs/valeurs propres $(\lambda_k, v_k)_{1 \leq k \leq r} \in (\mathbb{R}_+ \times \mathbb{C}^{nm})^r$ avec $r = mn$, de sorte que ¹³

$$C_\Phi = \sum_{k=1}^r v_k \lambda_k v_k^* = \sum_{k=1}^r w_k w_k^* \text{ en absorbant } \lambda_k \text{ dans } w_k := \sqrt{\lambda_k} v_k \in \mathbb{C}^{nm}$$

Maintenant, on peut utiliser l'isomorphisme $\mathbb{C}^{nm} \cong \mathbb{C}^n \otimes \mathbb{C}^m \cong \mathbb{M}_{m,n}(\mathbb{C})$ qui nous donne

$$w_k = \begin{bmatrix} w_{k,1} \\ \vdots \\ w_{k,n} \end{bmatrix} \mapsto W_k = \left[w_{k,1} \mid \cdots \mid w_{k,n} \right] \in \mathbb{M}_{m,n} \text{ avec } w_{k,i} \in \mathbb{C}^m$$

puis vérifier que Φ coïncide avec la transformation linéaire $A \in \mathbb{M}_n(\mathbb{C}) \mapsto \sum_{k=1}^r W_k A W_k^* \in \mathbb{M}_m$. En effet, elles coïncident sur la base $(E_{ij})_{1 \leq i, j \leq n}$ de $\mathbb{M}_n$:

D'une part, $\forall k \in [1, r], \forall i_0, j_0 \in [1, n]$,

$$W_k E_{i_0 j_0} W_k^* = \left[w_{k,1} \mid \cdots \mid w_{k,n} \right] \cdot [\mathbb{1}_{i_0 i_0} \mathbb{1}_{j_0 j_0}]_{i,j} \cdot \begin{bmatrix} w_{k,1}^* \\ \vdots \\ w_{k,n}^* \end{bmatrix} = w_{k,i_0} w_{k,j_0}^* \in \mathbb{M}_m$$

et d'autre part, on a la matrice par blocs

$$w_k w_k^* = \begin{bmatrix} w_{k,1} \\ \vdots \\ w_{k,n} \end{bmatrix} \cdot \left[w_{k,1}^* \mid \cdots \mid w_{k,n}^* \right] = \begin{bmatrix} w_{k,1} w_{k,1}^* & \cdots & w_{k,1} w_{k,n}^* \\ \vdots & \ddots & \vdots \\ w_{k,n} w_{k,1}^* & \cdots & w_{k,n} w_{k,n}^* \end{bmatrix} = [w_{k,i} w_{k,j}^*]_{1 \leq i, j \leq n} \in \mathbb{M}_{(nm)}$$

12. Il existe de nombreuses variations de cette preuve, certains plus formelles (par exemple [celle sur Wikipédia](#), qui utilise des projections π_i sur la i -ème copie de $\mathbb{C}^m$ dans $\mathbb{C}^{mn} \cong \bigotimes^n \mathbb{C}^m$), mais travailler directement avec des matrices par blocs a le mérite d'être plus visuel.

13. Ici, v_k^* désigne le vecteur ligne adjoint à v_k , matrice de la forme linéaire associée à v_k .

donc

$$\left[\sum_{k=1}^r W_k E_{ij} W_k^* \right]_{1 \leq i, j \leq n} = \sum_{k=1}^r [w_{k,i} w_{k,j}^*]_{i,j} = \sum_{k=1}^r w_k w_k^* = C_\Phi = [\Phi(E_{ij})]_{1 \leq i, j \leq n}$$

En identifiant les blocs, $\forall i, j \in \llbracket 1, n \rrbracket$, on a bien ce que l'on voulait :

$$\Phi(E_{ij}) = \sum_{k=1}^r W_k E_{ij} W_k^*$$

(d $\Rightarrow$ a) : C'est la proposition 6. □

Démonstration. de l'identité $\text{cr}(\Phi) = \text{rang}(C_\Phi)$.

- Dans la preuve (c $\Rightarrow$ d) ci-dessus, on effectue la décomposition de $C_\Phi = \sum_{k=1}^r v_k \lambda_k v_k^*$. On peut en fait toujours prendre $r = \text{rang}(C_\Phi)$ au lieu de mn , avec $\lambda_k = 0$ pour $k > r$. Ainsi, on n'a jamais besoin de plus de r opérateurs de Kraus : $\text{cr}(\Phi) \leq \text{rang}(C_\Phi)$.
- Maintenant, écrivons $\Phi = A \mapsto \sum_{k=1}^r W_k A W_k^*$. Majorons le rang de la matrice de Choi : on a

$$C_\Phi = [\Phi(E_{ij})]_{1 \leq i, j \leq n} = \left[\sum_{k=1}^r W_k E_{ij} W_k^* \right]_{i,j} = \sum_{k=1}^r \begin{bmatrix} W_k & & \\ & \ddots & \\ & & W_k \end{bmatrix} [E_{ij}]_{i,j} \begin{bmatrix} W_k^* & & \\ & \ddots & \\ & & W_k^* \end{bmatrix}$$

donc en utilisant les formules $\text{rang}(A+B) \leq \text{rang}(A) + \text{rang}(B)$ et $\text{rang}(AB) \leq \min(\text{rang}(A), \text{rang}(B))$,

$$\text{rang}(C_\Phi) \leq \sum_{k=1}^r \underbrace{\text{rang} \left(\begin{bmatrix} W_k & & \\ & \ddots & \\ & & W_k \end{bmatrix} [E_{ij}]_{i,j} \begin{bmatrix} W_k^* & & \\ & \ddots & \\ & & W_k^* \end{bmatrix} \right)}_{\leq 1} \leq r \quad \text{puisque} \quad \text{rang}([E_{ij}]_{i,j}) = 1$$

Ainsi, si on choisit $r = \text{cr}(\Phi)$ (nombre minimal d'opérateurs de Kraus), on a $\text{rang}(C_\Phi) \leq \text{cr}(\Phi)$. □

Remarque. Il existe d'autres façons de construire des opérateurs de Kraus pour Φ . En effet, si l'on effectue la décomposition $C_\Phi = B^* B$ de la matrice de Choi (qui est positive ; cette décomposition n'est d'ailleurs pas unique en général), et si on pose

$$B = \left[\begin{array}{c|c|c} b_1 & \cdots & b_{nm} \end{array} \right] \quad \text{avec} \quad b_k \in \mathbb{C}^{nm}, \quad \text{on a} \quad C_\Phi = \sum_{k=1}^{nm} b_k b_k^*$$

et on obtient des opérateurs de Kraus $(B_k)_{1 \leq k \leq nm}$ par le même argument que dans la preuve ci-dessus, mais en général différents des $(W_k)_{1 \leq k \leq nm}$, car les vecteurs $(b_k)_k$ n'ont aucune raison d'être orthogonaux, contrairement aux vecteurs $(w_k)_k$ obtenus par décomposition spectrale. Toutefois, comme on vient de le voir, c'est la décomposition spectrale qui minimise le nombre d'opérateurs de Kraus.

On peut se demander si la décomposition minimale en opérateurs de Kraus (avec $r = \text{cr}(\Phi)$) est unique. La réponse est négative. En effet, si on écrit $\Phi = A \mapsto \sum_{k=1}^r W_k A W_k^*$ et si on prend une matrice $r \times r$ unitaire $U = [u_{kl}]_{1 \leq k, l \leq r} \in \text{MU}_r(\mathbb{C})$, et que l'on pose $\forall k \in \llbracket 1, r \rrbracket$, $V_k := \sum_{l=1}^r u_{lk} W_l$, on a

$$\begin{aligned} \forall A \in \text{M}_n(\mathbb{C}), \quad \sum_{k=1}^r V_k A V_k^* &= \sum_{k=1}^r \left(\sum_{i=1}^r u_{ik} W_i \right) A \left(\sum_{j=1}^r \bar{u}_{jk} W_j^* \right) \\ &= \sum_{i=1}^r \sum_{j=1}^r \sum_{k=1}^r u_{ik} \bar{u}_{jk} W_i A W_j^* \\ [U^* &= [\bar{u}_{lk}]_{k,l}] &= \sum_{i=1}^r \sum_{j=1}^r (U U^*)_{ij} W_i A W_j^* \\ [U U^* &= 1 \text{ car } U \text{ unitaire}] &= \sum_{i=1}^r \sum_{j=1}^r \mathbb{1}_{ij} W_i A W_j^* = \sum_{i=1}^{nm} W_i A W_i^* = \Phi(A) \end{aligned}$$

Cette situation est en fait générale. En effet, on a le résultat suivant, que l'on admet [PM990, §4.2] :

Proposition 8. *Si $(V_k)_k, (W_k)_k \in (\mathbb{M}_{m,n}(\mathbb{C}))^r$ sont deux décompositions en opérateurs de Kraus de Φ , alors $\exists [u_{kl}]_{1 \leq k, l \leq r} \in \mathbb{M}_r(\mathbb{C})$ une matrice unitaire telle que*

$$\forall k \in \llbracket 1, r \rrbracket, \quad V_k = \sum_{l=1}^r u_{lk} W_l$$

2.4 Retour aux canaux quantiques

On est maintenant en mesure de répondre à la question centrale : *La condition de complète positivité est-elle suffisante pour que tout opérateur d'évolution soit un canal quantique ?*

Soient $\Phi_1 : \mathcal{L}(\mathcal{H}_{s,1}) \longrightarrow \mathcal{L}(\mathcal{H}_{o,1})$ et $\Phi_2 : \mathcal{L}(\mathcal{H}_{s,2}) \longrightarrow \mathcal{L}(\mathcal{H}_{o,2})$ deux transformations complètement positives et préservant la trace. On veut montrer que

$$\Phi_1 \otimes \Phi_2 : \mathcal{L}(\mathcal{H}_{s,1} \otimes \mathcal{H}_{s,2}) \longrightarrow \mathcal{L}(\mathcal{H}_{o,2} \otimes \mathcal{H}_{o,2})$$

est un opérateur d'évolution quantique, c'est à dire positif et préservant la trace. Pour que tout reste cohérent, on s'attend même à ce que $\Phi_1 \otimes \Phi_2$ soit complètement positif.

Proposition 9. *Soit $\Phi : \mathcal{L}(\mathcal{H}_1) \longrightarrow \mathcal{L}(\mathcal{H}_2)$ une transformation complètement positive, et*

$$\Phi = A \longmapsto \sum_{k=1}^r M_k A M_k^* \quad \text{avec} \quad (M_k)_{1 \leq k \leq r} \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)^r$$

n'importe quelle décomposition de Choi-Kraus de Φ . Alors

$$\Phi \text{ préserve la trace} \iff \sum_{k=1}^r M_k^* M_k = \mathbb{1}_{\mathcal{H}_1}$$

Démonstration.

$(\Leftarrow)$: $\forall A \in \mathcal{L}(\mathcal{H}_1)$, la trace de A est préservée car

$$\begin{aligned} \text{tr}(\Phi(A)) &= \text{tr} \left(\sum_{k=1}^r M_k A M_k^* \right) = \sum_{k=1}^r \text{tr}(M_k A M_k^*) = \sum_{k=1}^r \text{tr}(A M_k^* M_k) = \text{tr} \left(A \sum_{k=1}^r M_k^* M_k \right) \\ &= \text{tr}(A \mathbb{1}) = \text{tr}(A) \end{aligned}$$

$(\Rightarrow)$: Par préservation de la trace, et par le même calcul, on doit avoir $\forall A \in \mathcal{L}(\mathcal{H}_1)$,

$$\text{tr}(A) = \text{tr}(\Phi(A)) = \text{tr}(AU) \quad \text{avec} \quad U = \sum_{k=1}^r M_k^* M_k$$

En particulier, si on identifie matrice et opérateur, on a $\forall i, j \in \llbracket 1, n \rrbracket$ et pour $A = E_{ij}$,

$$\text{si } i \neq j : \quad 0 = \text{tr}(E_{ij}) = \text{tr}(E_{ij}U) = u_{ii}$$

$$\text{si } i = j : \quad 1 = \text{tr}(E_{ii}) = \text{tr}(E_{ii}U) = u_{ij}$$

avec $[u_{ij}]_{1 \leq i, j \leq n} = U$. Donc $U = \mathbb{1}_{\mathcal{H}_1}$. □

Ce que nous dit cette proposition ainsi que la caractérisation (8), c'est que tout opérateur d'évolution complètement positif $\Phi : \mathcal{L}(\mathcal{H}_s) \longrightarrow \mathcal{L}(\mathcal{H}_o)$ est représenté par un système de mesure $(M_k : \mathcal{H}_s \longrightarrow \mathcal{H}_o)_{1 \leq k \leq r}$ à r issues que l'on voit sous la forme (12), et toujours de façon non unique.

Ainsi, si l'on revient à nos transformations Φ_1 et Φ_2 , on peut écrire

$$\Phi_1 = A \longmapsto \sum_{k=1}^r M_{1,k} A M_{1,k}^* \quad \text{et} \quad \Phi_2 = B \longmapsto \sum_{k=1}^s M_{2,k} B M_{2,k}^*$$

Alors $\forall A \in \mathcal{L}(\mathcal{H}_{s,1}), \forall B \in \mathcal{L}(\mathcal{H}_{s,2})$, on observe que¹⁴

$$\begin{aligned}
(\Phi_1 \otimes \Phi_2)(A \otimes_s B) &= \left(\sum_{k=1}^r M_{1,k} A M_{1,k}^* \right) \otimes_o \left(\sum_{l=1}^s M_{2,l} B M_{2,l}^* \right) \\
[\text{isomorphisme (20)}] &= \sum_{k=1}^r \sum_{l=1}^s (M_{1,k} A M_{1,k}^*) \otimes_o (M_{2,l} B M_{2,l}^*) \\
&= \sum_{k=1}^r \sum_{l=1}^s (M_{1,k} \otimes_{s,o} M_{2,l}) (A \otimes_s B) (M_{1,k} \otimes_{s,o} M_{2,l})^*
\end{aligned}$$

Et comme la famille $\{A \otimes B : A \in \mathcal{L}(\mathcal{H}_{s,1}), B \in \mathcal{L}(\mathcal{H}_{s,2})\}$ génère $\mathcal{L}(\mathcal{H}_{s,1} \otimes \mathcal{H}_2)$, on en déduit que l'opérateur d'évolution couplée des systèmes 1 et 2 se met sous la forme

$$\Phi_1 \otimes \Phi_2 = C \mapsto \sum_{k=1}^r \sum_{l=1}^s M_{kl} C M_{kl}^* \quad \text{avec} \quad M_{kl} = M_{1,k} \otimes M_{2,l} \quad (24)$$

Donc par la proposition 6, $\Phi_1 \otimes \Phi_2$ est complètement positif. C'est en particulier une transformation positive! Enfin, la famille $(M_{kl} : \mathcal{H}_{s,1} \otimes \mathcal{H}_{s,2} \rightarrow \mathcal{H}_{s,2} \otimes \mathcal{H}_{o,2})_{1 \leq k \leq r, 1 \leq l \leq s}$ représente bien un système de mesure avec la proposition 9 car, de la même façon,

$$\begin{aligned}
\sum_{k=1}^r \sum_{l=1}^s M_{kl}^* M_{kl} &= \sum_{k=1}^r \sum_{l=1}^s (M_{1,k} \otimes M_{2,l})^* (M_{1,k} \otimes M_{2,l}) \\
&= \sum_{k=1}^r \sum_{l=1}^s (M_{1,k}^* M_{1,k}) \otimes (M_{2,l}^* M_{2,l}) \\
&= \left(\sum_{k=1}^r M_{1,k}^* M_{1,k} \right) \otimes \left(\sum_{l=1}^s M_{2,l}^* M_{2,l} \right) = \mathbb{1}_{\mathcal{H}_{s,1}} \otimes \mathbb{1}_{\mathcal{H}_{s,2}} = \mathbb{1}_{\mathcal{H}_{s,1} \otimes \mathcal{H}_{s,2}}
\end{aligned}$$

$\Phi_1 \otimes \Phi_2$ est donc bien un opérateur d'évolution : positif et préservant la trace, ce qui est équivalent (par le théorème 1) à dire que les opérateurs statistiques, représentant les mélanges d'états, sont envoyés sur des opérateurs de densité : $\forall P \in \mathcal{L}_{\text{tr}1}^+(\mathcal{H}_{s,1} \otimes \mathcal{H}_{s,2}), (\Phi_1 \otimes \Phi_2)(P) \in \mathcal{L}_{\text{tr}1}^+(\mathcal{H}_{s,2} \otimes \mathcal{H}_{o,2})$.

Corollaire 10. *Les canaux quantiques, en dimension finie, sont exactement les opérateurs d'évolution complètement positifs, c'est à dire les transformations linéaires $\mathcal{L}(\mathcal{H}_s) \rightarrow \mathcal{L}(\mathcal{H}_o)$ complètement positives préservant la trace (completely positive trace preserving, CPTP) :*

$$\text{CanauxQuantiques}(\mathcal{H}_s, \mathcal{H}_o) = \{ \Phi : \mathcal{L}(\mathcal{H}_s) \rightarrow \mathcal{L}(\mathcal{H}_o) \text{ CPTP} \}$$

3 Conclusion

On a ainsi identifié l'outil de base de la théorie quantique de l'information :

les transformations complètement positives préservant la trace, agissant sur des mélanges d'états

Il est à noter que cette notion, bien que très utilisée en théorie quantique de l'information ainsi qu'en informatique et communication quantique, n'est pas l'outil le plus général : on peut avoir à considérer

14. Si l'on veut être très explicite, par définition du produit tensoriel d'applications et par l'isomorphisme des Kronecker,

$$\begin{aligned}
(M_{1,k} A M_{1,k}^*) \otimes_o (M_{2,l} B M_{2,l}^*) &= M_{1,k}(A(M_{1,k}^*(\cdot_1))) \otimes_o M_{2,l}(B(M_{2,l}^*(\cdot_2))) \\
&= (M_{1,k} \otimes_{s,o} M_{2,l}) (A(M_{1,k}^*(\cdot_1)) \otimes_s B(M_{2,l}^*(\cdot_2))) \\
&= (M_{1,k} \otimes_{s,o} M_{2,l}) ((A \otimes_s B) (M_{1,k}^*(\cdot_1) \otimes_s M_{2,l}^*(\cdot_2))) \\
&= (M_{1,k} \otimes_{s,o} M_{2,l}) ((A \otimes_s B) ((M_{1,k}^* \otimes_{o,s} M_{2,l}^*)(\cdot_1 \otimes_o \cdot_2)))
\end{aligned}$$

et on vérifie que $M_{1,k}^* \otimes_{o,s} M_{2,l}^* = (M_{1,k} \otimes_{s,o} M_{2,l})^*$.

des transformations à trace décroissante, et éventuellement des applications non complètement positives si l'on accepte pas l'axiome 6 en toute généralité.

Les applications complètement positives disposent aussi d'un autre décomposition, donnée par le **théorème de dilatation de Stinespring**. Cette décomposition a l'avantage de se généraliser en dimension infinie, ce qui permet de généraliser notre conclusion en dimension infinie [Paulsen, 2003, th. 4.1] :

Théorème 11. Soient $\mathcal{A}$ une C^* -algèbre unitaire, $\mathcal{B}(\mathcal{H})$ l'algèbre des opérateurs bornés sur un espace de Hilbert $\mathcal{H}$, et une transformation complètement positive $\Phi : \mathcal{A} \rightarrow \mathcal{B}(\mathcal{H})$. Alors il existe un espace de Hilbert $\mathcal{K}$, un $*$ -morphisme unitaire $\pi : \mathcal{A} \rightarrow \mathcal{B}(\mathcal{K})$, et un opérateur borné $V : \mathcal{H} \rightarrow \mathcal{K}$ tel que

$$\forall A \in \mathcal{A}, \quad \Phi(A) = V^* \pi(A) V$$

À partir d'ici, on pourrait étudier les canaux de communication quantique (leur capacité, la correction d'erreurs, la compression et l'entropie) [Paulsen, 2016, Watrous, 2011], les mécanismes d'intrication quantique, l'algorithmique quantique, ou encore la théorie de la mesure quantique. Du point de vue mathématique, l'étude des applications complètement positives est toujours active [Poon, 2009].

Références

- Claude Aslangul. *Mécanique quantique - Tome 1 : Fondements et premières applications*. De Boeck, 2018. ISBN 9782807315556.
- D. Bertrand. Algèbre géométrique. Chapitre 4 : Géométrie multilinéaire, 2010. URL https://webusers.imj-prg.fr/~daniel.bertrand/Enseignement/epdf/Algeo09_chap4.pdf.
- Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3) :285–290, 1975. doi : 10.1016/0024-3795(75)90075-0.
- John Conway. *A course in functional analysis (2nd edition)*. Springer, 1990. ISBN 0-387-97245-5.
- Karl Kraus. *States, Effects, and Operations : Fundamental Notions of Quantum Theory (Lecture Notes in Physics)*. Springer, nov 1983. ISBN 978-3-5401-2732-1. URL <https://books.google.com/books?id=fRBBAQAATAAJ>.
- Michel Le Bellac. *Physique quantique - Tome 1 : Fondements*. EDP Sciences, 2013. ISBN 978-2-7598-0803-8.
- Vern Paulsen. *Completely Bounded Maps and Operator Algebras*. Cambridge University Press, 2003. ISBN 0521816696.
- Vern Paulsen. Entanglement and non-locality, P.Math 990 lecture notes, 2016. URL http://www.math.uwaterloo.ca/~vpaulsen/EntanglementAndNonlocality_LectureNotes_7.pdf.
- Yiu Tung Poon. Completely positive maps in quantum information, 2009. URL <http://www.math.unl.edu/~adonsig1/NIFAS/0911-Poon.pdf>.
- Marc Sage. Algèbre multilinéaire. URL <http://www.normalesup.org/~sage/Enseignement/Cours/ProdTens.pdf>.
- John Watrous. Theory of quantum information (lecture notes), 2011. URL <https://cs.uwaterloo.ca/~watrous/LectureNotes/CS766.Fall2011/all.pdf>.