Exposé de maîtrise

Caractériser l'intrication en mécanique quantique : le critère des frères Horodecki

Y. Luo, T. Nicolas
Encadrés par Thierry Paul

30 septembre 2008

Table des matières

1 Introduction

Dans ce texte, on se propose d'expliquer le critère des frères Horodecki caractérisant les états intriqués. On reviendra d'abord sur certaines notions utiles à la compréhension des enjeux du problème, comme les notions de matrice densité, de mélange statistique d'états, de produit tensoriel et d'intrication, préalablement à notre étude mathématique. Nous allons travailler en dimension finie dans un premier temps, et nous nous intéresserons dans la dernière section à une possible généralisation en dimension infinie des résultats établis.

2 Notions de base

2.1 Matrice densité d'un état, mélange statistique d'état

En mécanique quantique, il existe deux façons de représenter un état quantique : soit en tant qu'élément d'un espace de Hilbert H, auquel cas on le note $|\psi\rangle$, soit sous la forme de sa matrice densité notée ϱ, et telle que $\varrho = |\psi\rangle\langle\psi|$. On utilisera dans ce texte surtout cette dernière représentation, qui est celle d'un opérateur autoadjoint, positif et de trace 1. En fait, c'est la définition générale d'un état tel que nous les manipulerons dans ce texte. Précisons à ce point les notations.

Définition 1. *Si H est un espace de Hilbert, on note $\mathcal{L}(H)$ l'espace des applications linéaires continues de H dans H. On définit alors les sous-ensembles suivants de $\mathcal{L}(H)$:*

$$\mathcal{H}(H) = \left\{A \in \mathcal{L}(H) | A^\star = A\right\}$$

est l'espace des opérateurs autoadjoints.

$$\mathcal{H}^+(H) = \left\{A \in \mathcal{H}(H) | \sigma(A) \subset [0, +\infty[\right\}$$

est l'ensemble des opérateurs positifs.

$$\mathcal{P}(H) = \left\{P \in \mathcal{H}(H) | P^2 = P\right\}$$

est l'ensemble des projecteurs orthogonaux.

$$\mathcal{E}(H) = \left\{\varrho \in \mathcal{H}^+(H) | \mathrm{Tr}(\varrho) = 1\right\}$$

est l'ensemble des états.

D'après les définitions précédentes, un état de la forme $|\psi\rangle\langle\psi|$ est bien un élément de $\mathcal{E}(H)$. En effet, il est évident qu'un tel état est autoadjoint, par simple convention de notations. De plus cet état est le projecteur sur $|\psi\rangle$ et s'annule sur $|\psi\rangle^{\perp}$. Sa seule valeur propre non nulle est donc 1 avec multiplicité 1 et on a bien $\mathrm{Tr}(|\psi\rangle\langle\psi|) = 1$.

Ensuite, tout élément de la forme $\sum_{i=1}^{n} \lambda_i \varrho_i$, où ϱ_i est un état pur et $\sum_{i=1}^{n} \lambda_i = 1$, est également un état, la trace étant une opération linéaire. Ainsi, toute combinaison convexe d'états purs (ou de projecteurs orthogonaux de rang 1) est un état. Réciproquement, en diagonalisant un état ϱ, en notant λ_i la $i^{\text{ème}}$ valeur propre associée au vecteur propre $|\psi_i\rangle$, on a, dans une certaine base :

$$\varrho = \sum_{i=1}^{n} \lambda_i \varrho_i,$$

où $\varrho_i = |\psi_i\rangle\langle\psi_i|$.

Ainsi tout état est combinaison convexe d'états purs. On appelle ces états des états mixtes.

2.2 Produit tensoriel et intrication

Lorsque l'on dispose de deux espaces de Hilbert H_1 et H_2, on peut former leur produit tensoriel $H = H_1 \otimes H_2$. Un élément de H est alors de la forme $|\psi\rangle = \sum_{i,j} C_{ij} |i_1\rangle \otimes |j_2\rangle$, où $\{|i_1\rangle\}$ (resp $\{|j_2\rangle\}$) est une base de H_1 (resp H_2). On peut définir alors la notion d'intrication :

Définition 2 (Etat pur)**.** *Un état pur ϱ est dit **intriqué** s'il ne peut être mis sous la forme $\varrho = \varrho_1 \otimes \varrho_2$, avec ϱ_1 (resp ϱ_2) état sur H_1 (resp H_2), c'est-à-dire, avec $\varrho = |\psi\rangle\langle\psi|$, si $|\psi\rangle$ ne peut se mettre sous la forme $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ avec $|\psi_1\rangle, |\psi_2\rangle$ des états de H_1 et H_2. Dans le cas contraire, il est dit **séparable**.*

Dans le cas pur, la question de savoir si un état est intriqué ou pas est donc un problème mathématique assez simple, puisqu'il s'agit simplement, étant donné les nombres $\{C_{ij}\}$, de savoir s'il existe des nombres $\{a_i\}$ et $\{b_i\}$ tels qu'on ait : $C_{ij} = a_i b_j, \forall i, j$. (Cf. section 3.1).

Définition 3 (Cas général)**.** *Dans le cas général, on dit que l'état ϱ est intriqué s'il ne peut être approché, pour la norme induite par la trace, par des états de la forme*

$$\widetilde{\varrho} = \sum_{i,j} \lambda_{ij} \varrho_{1i} \otimes \varrho_{2j}, \tag{1}$$

avec $\varrho_{1i}, \varrho_{2j}$ des états respectivement sur H_1 et H_2, et $\sum_{i,j} \lambda_{ij} = 1$ par linéarité de la trace (un état doit être de trace 1). Si un état n'est pas intriqué, il est dit séparable, et on note $\mathcal{E}_s(H)$ l'ensemble des états séparables.

En termes plus précis, ϱ est séparable s'il existe une suite ϱ_n d'états de la forme (1) tels que $\varrho_n \longrightarrow \varrho$ en norme.

Attention aux confusions. Si $\{A_i\}_{1\leqslant i\leqslant m}$ et $\{B_j\}_{1\leqslant j\leqslant n}$ sont des bases des espaces de Hilbert $\mathcal{L}(H_1)$ et $\mathcal{L}(H_2)$, alors tout état sur $\mathcal{L}(H_1 \otimes H_2)$ s'écrit sous la forme $\sum_{i,j} \lambda_{ij} A_i \otimes B_j$. En revanche dans cette somme, A_i et B_j ne sont pas nécessairement des états. Par exemple, pour deux systèmes à deux niveaux, on a, pour l'état intriqué $|\psi\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$:

$$\varrho = \frac{1}{2}|0\rangle\langle 0| \otimes |1\rangle\langle 1| + \frac{1}{2}|0\rangle\langle 1| \otimes |1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 0| \otimes |0\rangle\langle 1| + \frac{1}{2}|1\rangle\langle 1| \otimes |0\rangle\langle 0|.$$

Dans cette somme, $|1\rangle\langle 0|$ et $|0\rangle\langle 1|$ ne sont pas des états (leur trace est nulle).

Maintenant que nous avons la notion d'intrication, précisons aussi le sens physique des états mixtes. Les états mixtes apparaissent naturellement lorsque, pour un système à plusieurs composantes, on veut obtenir de l'information sur une seule des composantes du système. On somme alors l'état par rapport aux degrés de liberté de toutes les composantes sauf une, et on obtient dans le cas général une matrice densité d'état mixte. Plus précisément, dans le cas d'un système à deux composantes par exemple, avec deux espaces de Hilbert H_1 et H_2 de dimensions m et n, et de bases $\{i_1\}_{1\leqslant i\leqslant m}$ et $\{j_2\}_{1\leqslant j\leqslant n}$, la trace partielle par rapport à la deuxième composante est définie comme :

$$\mathrm{Tr}_2(\varrho) = \sum_{j=1}^{n} \langle j_2|\varrho|j_2\rangle.$$

Ainsi, si ϱ est un état pur, et s'écrit donc $|\psi\rangle\langle\psi|$, où $|\psi\rangle$ est un élément de $H_1 \otimes H_2$, alors *a priori*, $\mathrm{Tr}_2(\varrho)$ est un état mixte, et il nous donne toute l'information disponible sur la première composante du système. On remarque d'ailleurs que si ϱ n'est pas intriqué, (il s'écrit donc $|\psi_1\rangle\langle\psi_1|\otimes|\psi_2\rangle\langle\psi_2|$), alors

$$\mathrm{Tr}_2(\varrho) = \sum_j |\psi_1\rangle\langle\psi_1|\langle j_2|\psi_2\rangle\langle\psi_2|j_2\rangle = |\psi_1\rangle\langle\psi_1|.$$

On vérifie donc bien que les deux composantes sont indépendantes.

Inversement, on peut aussi partir d'un état mixte quelconque ϱ_1 sur un espace de Hilbert H_1, et chercher s'il existe un espace de Hilbert H_2 et un état pur ϱ sur $H_1 \otimes H_2$ tels que $\varrho_1 = \mathrm{Tr}_2(\varrho)$. Trouver un tel espace de Hilbert revient à purifier le système. Ces considérations justifient l'intérêt porté aux états mixtes, et à la recherche d'un critère d'intrication. Or on va voir que dans le cas général d'état mixte, le problème de la caractérisation des états intriqués n'est pas trivial, malgré la simplicité des définitions données jusqu'ici.

3 Caractérisation des états séparables

3.1 Cas pur

On se donne ici un critère classique de la séparabilité des états purs. Il est plus pratique, dans le cas pur, de traiter le problème d'intrication avec simplement les notations de Dirac plutôt que les matrices de densité, puisque ces dernières décrivent dans la plupart des cas le comportement d'un mélange statistique d'états purs. Focalisons-nous d'abord sur le cas de dimension finie : notons $\{|e_i\rangle\}_{1\leq i\leq m}$ et $\{|f_i\rangle\}_{1\leq i\leq n}$ les bases respectives de H_1 et H_2, m et n étant leur dimension.

Proposition 1. *Un état pur $|\psi\rangle = \sum_{i,j} \lambda_{ij}|e_i\rangle \otimes |f_j\rangle$ est séparable si et seulement si la matrice $(\lambda_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ est de rang 1.*

Démonstration. D'après la définition précédente, un état pur séparable se décompose en $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, où $|\psi_1\rangle$ et $|\psi_2\rangle$ sont des états sur H_1 et H_2 respectivement. Si on note $|\psi_1\rangle = \sum_i \alpha_i|e_i\rangle$, $|\psi_2\rangle = \sum_j \beta_i|f_i\rangle$, et $|\psi\rangle = \sum_{i,j} \lambda_{ij}|e_i\rangle \otimes |f_j\rangle$, on a forcément pour tous $1 \leq i \leq m, 1 \leq j \leq n$,

$$\lambda_{ij} = \alpha_i\beta_j.$$

La matrice (λ_{ij}) est donc produit d'une matrice colonne et d'une matrice ligne, elle est donc de rang 0 ou 1. Or $(\alpha_i)_{1\leq i\leq m}$ et $(\beta_j)_{1\leq j\leq n}$ sont non nulles car les coefficients vérifient $\sum_i \alpha_i^2 = 1$ et $\sum_i \beta_i^2 = 1$, donc leur produit matriciel est non nul : (λ_{ij}) est donc de rang 1.

Réciproquement, si $M = \{\lambda_{ij}\}$ est de rang 1 et verifie $\sum_{i,j} \lambda_{ij}^2 = 1$, on peut considérer M comme une application de H_2 dans H_1 ; comme son image est de dimension 1 selon l'hypothèse, on peut prendre $|\psi_1\rangle = \sum_i \alpha_i|e_i\rangle \in H_1$ qui l'engendre. On peut supposer de plus que $\sum_i \alpha_i^2 = 1$, quitte à normaliser ce vecteur. $\square$

On note ensuite, pour $1 \leq j \leq n$, $\beta_j = \langle M \cdot f_j|\psi_1\rangle$.
Comme $\mathrm{Im}(M) = \mathrm{Vect}(\psi_1)$, $M \cdot f_j \in \mathrm{Vect}(\psi_1)$, donc on a

$$\forall 1 \leq j \leq n,\ |M \cdot f_j\rangle = \beta_j|\psi_1\rangle.$$

On vérifie que $\lambda_{ij} = \alpha_i\beta_j$:

$$\begin{aligned} \lambda_{ij} &= \langle M \cdot f_j|e_i\rangle \\ &= \beta_j\langle\psi_1|e_i\rangle \\ &= \beta_j \cdot \alpha_i \end{aligned}$$

Enfin on remarque que

$$\sum_{i,j} \lambda_{ij}^2 \;=\; \sum_{i,j} \alpha_i^2 \beta_j^2 = (\sum_i \alpha_i^2)(\sum_j \beta_j^2).$$

Ainsi $\sum_{i,j} \lambda_{ij}^2 = 1$ et $\sum_i \alpha_i^2 = 1$ implique $\sum_j \beta_j^2 = 1$.
On note $|\psi_2\rangle = \sum_j \beta_j |f_j\rangle$, et on en conclut que $|\psi\rangle = \sum_{i,j} \lambda_{ij} |e_i\rangle \otimes |f_j\rangle$ s'écrit comme $|\psi_1\rangle \otimes |\psi_2\rangle$, $|\psi_1\rangle$ et $|\psi_2\rangle$ étant bien des états dans H_1 et H_2, donc $|\psi\rangle$ est un état séparable.

Ce critère s'étend au cas où H_1 et H_2 sont des espaces de Hilbert *séparables*, puisque la notion de rang se généralise en dimension infinie, et la démonstration reste valable pour des bases hilbertiennes dénombrables de H_1 et H_2.

Néanmoins, il s'avère sans effet quant au cas d'états mixtes, pour la simple raison que la somme des deux matrices de rang 1 n'est *a priori* pas de rang 1. Dans la suite, on se propose d'étudier un critère de séparabilité plus global, le critère de *Horodecki*, qui restera valable pour les états mixtes.

3.2 Applications Positives et Complètement Positives

Nous allons avoir besoin des notions d'applications Positives et Complètement Positives dans notre discussion. On note $\mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$ l'espace des applications linéaires continues de $\mathcal{L}(H_1)$ dans $\mathcal{L}(H_2)$.

Définition 4. *Une application $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$ est dite* ***positive*** *si on a $\Lambda(\mathcal{H}^+(H_1)) \subset \mathcal{H}^+(H_2)$. Ensuite Λ est dite* ***complètement positive*** *si l'application induite*

$$\Lambda_n = \mathbb{I}_n \otimes \Lambda : \mathbb{M}_n \otimes \mathcal{L}(H_1) \to \mathbb{M}_n \otimes \mathcal{L}(H_2)$$

est positive pour tout n.

Dans cette définition, $\mathbb{I}_n$ désigne l'identité sur l'espace $\mathbb{M}_n$ des matrices carrées de dimension n. Cette définition a bien un sens. En effet l'espace $\mathbb{M}_n$ des matrices carrées de dimension n, muni de son produit scalaire canonique, est bien un espace de Hilbert, on peut donc réaliser son produit tensoriel avec l'espace de Hilbert $\mathcal{L}(H_1)$, qui est à son tour un espace de Hilbert, dans lequel on peut donc définir la notion d'opérateur positif. Bien entendu, toute application complètement positive est aussi positive. En revanche, il existe des applications positives qui ne sont pas complètement positives. Nous allons en développer un exemple qui sera capital pour la suite. Il s'agit de l'application de transposition :

$$\begin{array}{rcl} T : \mathcal{L}(H_1) & \longrightarrow & \mathcal{L}(H_1) \\ \varrho & \longmapsto & \varrho^T \end{array}$$

On a que T est positive, car si ϱ est un opérateur positif (on notera désormais $\varrho \geqslant 0$), alors en particulier $T(\varrho) = \varrho^T \geqslant 0$. En revanche $(\mathbb{I} \otimes T)$ n'est pas une application positive, donc T n'est pas complètement positive. En effet, on peut exhiber un exemple d'opérateur positif dont l'image n'est plus un opérateur positif. Soit, dans le cas où $H_1 = H_2$ est un espace de Hilbert de dimension finie N et de base $\{|1\rangle, \dots |N\rangle\}$, l'état $|\psi_+\rangle$ défini par :

$$|\psi_+\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle \otimes |i\rangle.$$

Sa matrice densité est le projecteur orthogonal

$$\begin{aligned} P_+ &= \frac{1}{N} \sum_{i,j} (|i\rangle \otimes |i\rangle)(\langle j| \otimes \langle j|) \\ &= \frac{1}{N} \sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle j| \end{aligned}$$

On a donc $(\mathbb{I} \otimes T)P_+ = \frac{1}{N} \sum_{i,j} |i\rangle\langle j| \otimes |j\rangle\langle i|$ dont il est facile de montrer que les valeurs propres sont 1 et -1 et qui n'est donc pas un opérateur positif.

Donnons maintenant la caractérisation suivante des applications positives, qui nous sera utile par la suite :

Lemme 2. $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$ *est une application positive si et seulement si on a :*

$$\forall P_1 \in \mathcal{P}(H_1), P_2 \in \mathcal{P}(H_2), \quad \mathrm{Tr}\big(\Lambda(P_1)P_2\big)) \geqslant 0.$$

Démonstration. Supposons que Λ est positive : soit $P_1 \in \mathcal{P}(H_1), P_2 \in \mathcal{P}(H_2)$. On sait que $P_1 \in \mathcal{P}(H_1) \subset \mathcal{H}^+(H_1)$ donc $\Lambda(P_1) \in \mathcal{H}^+(H_2)$. Or, une caractérisation d'opérateur positif sur H est :

$$Q \in \mathcal{H}^+(H) \Leftrightarrow \forall P \in \mathcal{P}(H), \quad \mathrm{Tr}(PQ) \geqslant 0.$$

D'où $\mathrm{Tr}\big(\Lambda(P_1)P_2\big) \geqslant 0$.

Réciproquement, soit $Q \in \mathcal{H}^+(H_1)$. Q se diagonalise dans une base de vecteurs propres $\{|i\rangle\}$ avec les valeurs propres associées (λ_i), les λ_i étant toutes positives. Q s'écrit donc comme

$$Q = \sum_i \lambda_i P_i,$$

avec $P_i = |i\rangle\langle i|$ des projecteurs orthogonaux de dimension 1 sur H_1. Or, on sait que $\forall P' \in \mathcal{P}(H_2),\ \ \mathrm{Tr}\big(\Lambda(P_i)P'\big) \geqslant 0$. Par linéarité de la trace, on obtient $\forall P' \in \mathcal{P}(H_2),\ \ \mathrm{Tr}\big(\Lambda(Q)P'\big) \geqslant 0$. D'après la caractérisation des opérateurs positifs, $\Lambda(Q)$ est positive. □

L'idée essentielle en ce qui concerne l'intrication est la suivante : soit Λ une application positive, complètement positive ou non. Soit ϱ un état séparable. Par définition, on peut approcher ϱ par des états de la forme

$$\sum_i p_i \varrho_{i1} \otimes \varrho_{i2},$$

dont l'image par $(\mathbb{I} \otimes \Lambda)$ est

$$\sum_i p_i \varrho_{i1} \otimes \Lambda(\varrho_{i2}).$$

qui est trivialement toujours un opérateur positif. On peut alors espérer obtenir un critère de séparabilité satisfaisant en trouvant une application positive non complètement positive Λ telle que $(\mathbb{I} \otimes \Lambda)$ ne transforme pas les états intriqués en opérateurs positifs. Une telle application pourra dépendre de l'état, et c'est aussi ce qui complique le problème. Pour les faibles dimensions (systèmes $2 \otimes 2$ et $2 \otimes 3$), le problème est entièrement résolu, et il se trouve que l'application $\Lambda = T$ est d'un intérêt capital, comme nous le verrons par la suite.

Notre but est de démontrer le théorème suivant, dû à *M, P. et R. Horodecki*. Un état ϱ sur $H_1 \otimes H_2$ est séparable si et seulement si, pour toute application positive $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$, l'opérateur $(I \otimes \Lambda)\varrho$ est un opérateur positif sur $H_1 \otimes H_1$.

3.3 Premier critère

Pour démontrer ce théorème, il va nous falloir établir quelques résultats préliminaires. Plus précisément, on a la proposition suivante.

Proposition 3. *Un état ϱ est séparable si et seulement si pour tout A élément de $\mathcal{L}(H)$ vérifiant* $\mathrm{Tr}(A\sigma) \geqslant 0$ *pour $\sigma \in \mathcal{E}_s(H)$, on a :* $\mathrm{Tr}(A\varrho) \geqslant 0$*, c'est à dire :*

$$\varrho \in \mathcal{E}_s(H) \iff \forall A \in \mathcal{L}(H), \Big(\mathrm{Tr}(A\sigma) \geqslant 0 \; \forall \sigma \in \mathcal{E}_s(H) \Longrightarrow \mathrm{Tr}(A\varrho) \geqslant 0\Big).$$

Démonstration. Commençons par montrer que l'espace des états séparables, noté $\mathcal{E}_s(H)$ est un convexe de $\mathcal{L}(H)$. Avec la définition que nous avons donnée, qui est qu'un état est séparable s'il est approchable par des états de la forme $\widetilde{\varrho} = \sum_i^n \lambda_i \varrho_{1i} \otimes \varrho_{2i}$, on voit que tout état de la forme $t\varrho' + (1-t)\varrho''$, avec $t \in [0,1]$, et ϱ', ϱ'' deux états séparables, est encore approchable par la somme pondérée des approximations de ϱ' et ϱ'', donc séparable. $\mathcal{E}_s(H)$ est donc bien convexe.

Une autre façon plus synthétique de le voir est de remarquer que, avec notre définition, $\mathcal{E}_s(H)$ est l'enveloppe convexe fermée de l'ensemble

$$\big\{\varrho_1 \otimes \varrho_2 | (\varrho_1, \varrho_2) \in \mathcal{E}(H_1) \times \mathcal{E}(H_2)\big\}.$$

L'enveloppe convexe fermée d'un ensemble quelconque est bien convexe.

Pour finir la démonstration, il suffira alors simplement d'appliquer le théorème d'Hahn-Banach[1], mais avant de l'expliciter, comme il s'agit de géométrie réelle dans un espace complexe, il faut préciser le rapport entre le produit scalaire hermitien induit par la trace et les formes affines réelles :

Lemme 4. *Soit φ une forme réelle affine sur $\mathcal{L}(H)$. Alors, on a :*

$$\exists A \in \mathcal{H}(H), \forall \varrho \in \mathcal{E}(H), \varphi(\varrho) = \mathrm{Tr}(A\varrho).$$

Démonstration. Si φ est une forme affine réelle, alors, à une constante réelle α près, c'est la partie réelle d'une forme linéaire complexe ψ. Grâce au produit scalaire induit par la norme, on a :

$$\exists \widetilde{A} \in \mathcal{L}(H),\, \forall \varrho \in \mathcal{L}(H),\, \psi(\varrho) = \langle \widetilde{A}, \varrho \rangle = \mathrm{Tr}(\widetilde{A}^* \varrho).$$

Soit maintenant $\varrho \in \mathcal{E}(H)$. Puisque ϱ est autoadjoint, on a

$$\varphi(\varrho) - \alpha = \mathrm{Re}\Big(\mathrm{Tr}(\widetilde{A}^*\varrho)\Big) = \frac{1}{2}\mathrm{Tr}(\widetilde{A}^*\varrho + A\varrho^*) = \mathrm{Tr}\left[\frac{\widetilde{A}^* + A}{2}\varrho\right].$$

Donc $(\widetilde{A}^* + A)/2 + \alpha \mathrm{Id}$ convient. □

[1] En dimension finie, il n'est bien sûr pas nécessaire d'invoquer ce théorème, mais cette étape resterait vraie en dimension infinie, et nous n'aurons donc pas besoin d'y revenir.

Terminons maintenant la preuve de la proposition 3. La condition nécessaire est tautologique. Pour montrer la condition suffisante, on applique le théorème d'Hahn-Banach. On raisonne par contraposée.

Soit ϱ un état non séparable. $\mathcal{E}_s(H)$ étant un convexe fermé et $\{\varrho\}$ un compact, d'après le théorème d'Hahn-Banach, $\mathcal{E}_s(H)$ et $\{\varrho\}$ sont séparés strictement par un hyperplan. Il existe donc une forme linéaire réelle ϕ et un réel α tels que $\phi(\sigma) > \alpha$ sur $\mathcal{E}_s(H)$ et $\phi(\varrho) < \alpha$, donc une forme affine φ telle que $\varphi(\sigma) > 0$ sur $\mathcal{E}_s(H)$ et $\varphi(\varrho) < 0$. D'après le résultat précédent,

$$\exists A \in \mathcal{L}(H), \forall \varrho \in \mathcal{E}(H), \varphi(\varrho) = \mathrm{Tr}(A\varrho),$$

et on a donc

$$\mathrm{Tr}(A\sigma) \geq 0, \forall \sigma \in \mathcal{E}_s(H) \text{ et } \mathrm{Tr}(A\varrho) < 0,$$

ce qui est la négation du membre de droite de l'équivalence. □

Proposition 5. *Soit A un opérateur sur $\mathcal{L}(H)$. Alors on a l'équivalence suivante :*

$$\forall \varrho \in \mathcal{E}_s(H), \mathrm{Tr}(A\varrho) \geqslant 0 \Longleftrightarrow \forall P_1 \in \mathcal{P}(H_1), \forall P_2 \in \mathcal{P}(H_2), \mathrm{Tr}\big(A(P_1 \otimes P_2)\big) \geqslant 0.$$

Démonstration. Ceci est simple : pour montrer la condition nécessaire, il suffit de remarquer que pour tout couple de projecteurs (P_1, P_2), $\frac{P_1 \otimes P_2}{\mathrm{Tr}(P_1)\mathrm{Tr}(P_2)}$ est un état, car de trace 1. Par linéarité de la trace, on a bien $\mathrm{Tr}\big(A(P_1 \otimes P_2)\big) \geqslant 0$.

Pour montrer la condition suffisante, montrons que la propriété est vraie pour tout état de la forme $\varrho_1 \otimes \varrho_2$ où ϱ_1 et ϱ_2 sont des états sur H_1 et H_2. Par la définition de $\mathcal{E}_s(H)$ (enveloppe convexe fermée de l'ensemble de ces états), et par la linéarité de la trace, on aura bien le résultat. Or ϱ_1 et ϱ_2 sont tous deux combinaisons convexes de projecteurs de rang 1, donc leur produit tensoriel également : si $\varrho_1 = \sum_i \lambda_i P_i$ et $\varrho_2 = \sum_j \mu_j P_j$ alors, on a :

$$\varrho_1 \otimes \varrho_2 = \sum_{i,j} \lambda_i \mu_j P_i \otimes P_j,$$

$$\text{avec } \sum_{i,j} \lambda_i \mu_j = 1.$$

Donc, toujours par linéarité de la trace, on a

$$\mathrm{Tr}\big(A(\varrho_1 \otimes \varrho_2)\big) \geqslant 0.$$

□

Nous allons voir ce que devient cette condition à la lumière d'un isomorphisme entre $\mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$ et $\mathcal{L}(H_1 \otimes H_2)$.

Proposition 6. *Il existe un isomorphisme S de $\mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$ dans $\mathcal{L}(H_1 \otimes H_2)$ tel que pour tous $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$, $A \in \mathcal{L}(H_1)$ et $B \in \mathcal{L}(H_2)$, on ait $\mathrm{Tr}\big(S(\Lambda)(A \otimes B)\big) = \mathrm{Tr}\big(\Lambda(A)B\big)$.*

Démonstration. Définissons S, puis nous montrerons qu'il s'agit bien d'un isomorphisme. Soit $\varrho \in \mathcal{L}(H_1 \otimes H_2)$, $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$. ϱ se décompose en somme de produits tensoriels d'opérateurs sur H_1 et H_2 : $\sum_{i,j} \lambda_{ij} A_i \otimes B_j$, où $\{A_i\}$ et $\{B_j\}$ sont les bases de $\mathcal{L}(H_1)$ et $\mathcal{L}(H_2)$. Alors l'application

$$\begin{array}{rcl} \Phi_\Lambda : \mathcal{L}(H_1 \otimes H_2) & \longrightarrow & \mathbb{C} \\ \varrho & \longmapsto & \displaystyle\sum_{i,j} \lambda_{ij} \mathrm{Tr}\big(\Lambda(A_i)B_j\big) \end{array}$$

est une forme linéaire manifestement continue (on est en dimension finie), donc admet une représentation à l'aide du produit scalaire sur $\mathcal{L}(H_1 \otimes H_2)$:

$$\forall \Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big), \exists!\, R(\Lambda), \forall \varrho \in \mathcal{L}(H_1 \otimes H_2),$$
$$\Phi_\Lambda(\varrho) = \langle R(\Lambda), \varrho \rangle = \mathrm{Tr}(R(\Lambda)^* \varrho).$$

On définit alors

$$\begin{array}{rcl} S : \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big) & \longrightarrow & \mathcal{L}(H_1 \otimes H_2) \\ \Lambda & \longmapsto & R(\Lambda)^* \end{array}$$

Le choix de $R(\Lambda)^*$ vient du fait que $R(\Lambda)$ dépend antilinéairement de Λ, donc $R(\Lambda)^*$ en dépend linéairement. En effet, on a d'une part, pour tous $\Lambda, \Gamma \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$ et $\varrho \in \mathcal{L}(H_1 \otimes H_2)$:

$$\begin{array}{rcl} \Phi_{\Lambda+\Gamma}(\varrho) & = & \displaystyle\sum_{i,j} \lambda_{ij} \mathrm{Tr}\big(\Lambda(A_i)B_j\big) + \sum_{i,j} \lambda_{ij} \mathrm{Tr}\big(\Gamma(A_i)B_j\big) \\ & = & \mathrm{Tr}(R(\Lambda)^* \varrho) + \mathrm{Tr}(R(\Gamma)^* \varrho) \\ & = & \mathrm{Tr}(R(\Lambda + \Gamma)^* \varrho) \end{array}$$

et d'autre part, pour tout $\alpha \in \mathbb{C}$,

$$\begin{array}{rcl} \Phi_{\alpha\Lambda}(\varrho) & = & \alpha \displaystyle\sum_{i,j} \lambda_{ij} \mathrm{Tr}\big(\Lambda(A_i)B_j\big) \\ & = & \alpha \mathrm{Tr}(R(\Lambda)^* \varrho) \\ & = & \mathrm{Tr}((\alpha^* R(\Lambda))^* \varrho) \\ & = & \mathrm{Tr}(R(\alpha\Lambda)^* \varrho) \end{array}$$

Ceci étant vrai pour tout opérateur ϱ, on a bien :

$$R(\Lambda + \Gamma) = R(\Lambda) + R(\Gamma) \quad \text{et} \quad R(\alpha\Lambda) = \alpha^* R(\Lambda),$$

et par conséquent

$$S(\Lambda + \Gamma) = S(\Lambda) + S(\Gamma) \quad \text{et} \quad S(\alpha\Lambda) = \alpha S(\Lambda).$$

L'application S est donc bien linéaire. De plus on a bien, pour tous $A \in \mathcal{L}(H_1)$ et $B \in \mathcal{L}(H_2)$, $\mathrm{Tr}\big(S(\Lambda)(A \otimes B)\big) = \mathrm{Tr}\big(\Lambda(A)B\big)$. Ceci vient du fait que A et B se décomposent tous deux sur la base de $\mathcal{L}(H_1)$ et de $\mathcal{L}(H_2)$ avec des coefficients $\{a_i\}$ et $\{b_j\}$. Par la définition de S, il vient que

$$\mathrm{Tr}\big(S(\Lambda)(A \otimes B)\big) = \sum_{i,j} a_i b_j \mathrm{Tr}(\Lambda(A_i)B_j) = \mathrm{Tr}\big(\Lambda(A)B\big).$$

Il reste à vérifier qu'il s'agit bien d'un isomorphisme.

L'injectivité est facile à prouver. Si $S(\Lambda) = S(\Gamma)$, alors, pour tous $A \in \mathcal{L}(H_1)$ et $B \in \mathcal{L}(H_2)$, on a $\mathrm{Tr}(\Lambda(A)B) = \mathrm{Tr}(\Gamma(A)B)$, donc $\Lambda(A) = \Gamma(A)$, $\forall A \in \mathcal{L}(H_1)$, donc $\Lambda = \Gamma$.

La surjectivité est également aisée à démontrer. On peut en effet exhiber, pour $\varrho \in \mathcal{L}(H_1 \otimes H_2)$, $S^{-1}(\varrho)$. Il suffit de le réaliser sur la base des $\{A_i \otimes B_j\}$ de $\mathcal{L}(H_1 \otimes H_2)$. On voit qu'en posant $\Lambda_{ij} : A \longmapsto \mathrm{Tr}(A_i A)B_j$ l'application qui envoie A_i^* sur B_j, on a

$$\mathrm{Tr}((A_i \otimes B_j)(A \otimes B)) = \mathrm{Tr}(A_i A)\mathrm{Tr}(B_j B) = \mathrm{Tr}(\Lambda_{ij}(A)B).$$

Donc $S(\Lambda_{ij}) = A_i \otimes B_j$ (en effet, cela étant vrai quels que soient les opérateurs A et B, $A_i \otimes B_j$ ne peut pas être différent de $S(\Lambda_{ij})$). S est donc bien un isomorphisme entre $\mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$ et $\mathcal{L}(H_1 \otimes H_2)$, qui vérifie bien la propriété demandée. $\square$

Nous avons donc obtenu la caractérisation suivante des états séparables :

Proposition 7. *Un état ϱ est séparable si et seulement si pour toute application positive Λ de $\mathcal{L}(H_1)$ dans $\mathcal{L}(H_2)$, on a $\mathrm{Tr}\big(S(\Lambda)\varrho\big) \geqslant 0$.*

Démonstration. Les équivalences suivantes découlent de tout ce qui précède, en particulier le lemme 2 :

$$\begin{aligned}
\varrho \in \mathcal{E}_s(H) \iff & \forall A \in \mathcal{L}(H), \Big(\mathrm{Tr}(A\sigma) \geqslant 0 \text{ sur } \mathcal{E}_s(H) \Longrightarrow \mathrm{Tr}(A\varrho) \geqslant 0\Big) \\
\iff & \forall A \in \mathcal{L}(H), \Big(\mathrm{Tr}(AP_1 \otimes P_2) \geqslant 0 \ \forall P_1, P_2 \in \mathcal{P}(H_1), \mathcal{P}(H_2) \\
& \qquad\qquad \Longrightarrow \mathrm{Tr}(A\varrho) \geqslant 0\Big) \\
\iff & \forall A \in \mathcal{L}(H), \Big(\mathrm{Tr}(S^{-1}(A)(P_1)P_2) \geqslant 0 \ \forall P_1, P_2 \in \mathcal{P}(H_1), \mathcal{P}(H_2) \\
& \qquad\qquad \Longrightarrow \mathrm{Tr}(A\varrho) \geqslant 0\Big) \\
\iff & \forall A \in \mathcal{L}(H), \Big(S^{-1}(A) \text{ positive} \Longrightarrow \mathrm{Tr}(A\varrho) \geqslant 0\Big) \\
\iff & \forall \Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big), \Big(\Lambda \text{ positive} \Longrightarrow \mathrm{Tr}\big(S(\Lambda)\varrho\big) \geqslant 0\Big).
\end{aligned}$$

□

Ceci démontre la proposition. Cependant ce critère n'est pas bien exploitable car, à ce stade, on ne connaît pas bien l'isomorphisme S. Nous allons donc maintenant nous atteler à ce problème pour arriver à la caractérisation des états séparables proposée par les frères Horodecki.

3.4 Le critère des frères Horodecki

3.4.1 Détermination de l'isomorphisme S

Proposition 8. *Il existe un unique élément U de $\mathcal{L}(H_1 \otimes H_1)$ tel que, pour tous $A, A' \in \mathcal{L}(H_1)$, on ait $\mathrm{Tr}\big(U(A \otimes A')\big) = \mathrm{Tr}(AA')$.*

Démonstration. Ce résultat découle directement de la proposition 6. En effet on remarque que si $H_1 = H_2$, alors, en notant $\mathbb{I}_1$ l'identité de $\mathcal{L}(H_1)$, on a $U = S(\mathbb{I}_1)$.

On peut de plus totalement expliciter l'application U. En notant $\{|i\rangle\}_{1 \leqslant i \leqslant n}$ une base de H_1, on peut se convaincre que l'opérateur

$$U = \sum_{i,j} |i\rangle\langle j| \otimes |j\rangle\langle i|$$

satisfait la proposition.

En effet, soit $A, A' \in \mathcal{L}(H_1)$, alors A (resp. A') se décompose sur la base orthonormée de $\mathcal{L}(H_1)$ formée par les opérateurs $|i\rangle\langle j|$, avec des coefficients notés λ_{ij} (resp. μ_{ij}).

$$\begin{aligned}
\mathrm{Tr}\big(U(A \otimes A')\big) &= \sum_{i,j} \mathrm{Tr}\big(|i\rangle\langle j|A \otimes |j\rangle\langle i|A'\big) \\
&= \sum_{i,j} \mathrm{Tr}\big(|i\rangle\langle j|A\big)\mathrm{Tr}\big(|j\rangle\langle i|A'\big).
\end{aligned}$$

On vérifie alors par des calculs élémentaires que $\mathrm{Tr}\big(|i\rangle\langle j|A\big) = \lambda_{ji}$, donc $\mathrm{Tr}\big(U(A \otimes A')\big) = \sum_{ij} \lambda_{ij}\mu_{ji}$ (les indices sont muets), qui est bien égale à $\mathrm{Tr}(AA')$. $\square$

Il ne reste plus qu'à établir l'unicité. On remarque d'abord que les opérateurs du type $A \otimes A'$, pour $A, A' \in \mathcal{L}(H_1)$ engendrent $\mathcal{L}(H_1 \otimes H_1)$. Ainsi par linéarité de la trace,

$$\begin{array}{rcl}
\Phi : \mathcal{L}(H_1) \otimes \mathcal{L}(H_1) & \longrightarrow & \mathbb{C} \\
A \otimes A' & \longmapsto & Tr(AA')
\end{array}$$

induit une forme linéaire sur $\mathcal{L}(H_1 \otimes H_1)$. Comme le produit scalaire associé à la norme trace fait de $\mathcal{L}(H_1 \otimes H_1)$ un espace de Hilbert, on en déduit l'existence et surtout l'unicité d'un opérateur $U \in \mathcal{L}(H_1 \otimes H_1)$ tel que

$$\forall A \in \mathcal{L}(H_1 \otimes H_1), \Phi(A) = \mathrm{Tr}(UA).$$

Notamment, pour tout $A \otimes A', \Phi(A \otimes A') = \mathrm{Tr}\big(U(A \otimes A')\big) = \mathrm{Tr}(AA')$.

Une propriété intéressante de la matrice U est qu'elle ne dépend pas du choix de la base de $\mathcal{L}(H_1)$. Pour s'en convaincre, on pourra vérifier que pour toute matrice de changement de bases orthonormées Q de H_1 sur H_1 on a :

$$(Q^* \otimes Q^*)U(Q \otimes Q) = U.$$

Pour faire cela, il suffit de vérifier à l'aide de calculs élémentaires que l'action de $(Q \otimes Q)U$ sur les vecteurs de base de $H_1 \otimes H_1$ (de la forme $|i\rangle \otimes |j\rangle$), est la même que celle de $U(Q \otimes Q)$, à savoir :

$$\sum_{k,l} \lambda_{jk}\lambda_{il}|k\rangle \otimes |l\rangle,$$

où les λ_{ij} sont les coefficients du changement de base : $Q|i\rangle = \sum_j \lambda_{ij}|j\rangle$.

Cette application U, obtenue à partir de S, permet en retour de caractériser cet isomorphisme. On a la proposition suivante :

Proposition 9. *Soit* $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$. *Alors*

$$S(\Lambda) = (I \otimes \Lambda)U.$$

Démonstration. Soit $(A, B) \in \mathcal{L}(H_1) \times \mathcal{L}(H_2)$. Alors :

$$\begin{aligned}
\mathrm{Tr}\big((I \otimes \Lambda)U(A \otimes B)\big) &= \langle A^* \otimes B^*, (I \otimes \Lambda)U\rangle = \langle (I \otimes \Lambda^*)(A^* \otimes B^*), U\rangle \\
&= \langle A^* \otimes \Lambda^*(B^*), U\rangle = \mathrm{Tr}\big(U(A \otimes \Lambda^*(B^*)^*)\big) \\
&= \mathrm{Tr}\big(\Lambda^*(B^*)^* A\big) = \langle \Lambda^*(B^*), A\rangle = \langle B^*, \Lambda(A)\rangle \\
&= \mathrm{Tr}\big(\Lambda(A)B\big) = \mathrm{Tr}\big(S(\Lambda)(A \otimes B)\big).
\end{aligned}$$

□

Remarquons que cela est tout à fait cohérent avec ce que l'on avait trouvé précedemment dans la preuve de la proposition 6, bien que nos notations aient été différentes : on vérifiera, en adaptant les notations, en prenant sur H_1 la base orthonormée des $A_{ij} = |i\rangle\langle j|$ (et sur H_2 la base correspondante d'élément générique noté B_{ij}), et en utilisant la caractérisation de S que l'on vient d'obtenir, que l'on a :

$$S(\Lambda_{ij\,k\,l}) = A_{ij} \otimes B_{kl},$$

où $\Lambda_{ij\,k\,l}$ est l'application qui envoie $|j\rangle\langle i|$ sur $|k\rangle\langle l|$, ce qui est bien le résultat que l'on avait trouvé.

Maintenant que l'on connaît S, on va pouvoir exprimer notre critère de séparabilité d'une manière plus élégante.

3.4.2 Le critère de Horodecki

Avant d'en arriver au théorème des frères Horodecki, il reste deux petits lemmes à établir.

Lemme 10. *Soit* $C \in \mathcal{H}^+(H_1 \otimes H_1)$. *Alors* $\mathrm{Tr}(UC) \geqslant 0$.

Démonstration. Comme C est un opérateur positif, il existe une base orthonormée (encore notée $\{|i\rangle\langle j|\}$) dans laquelle C est diagonale, et donc s'écrit :

$$C = \sum_{i,j} \lambda_{ij} |i\rangle\langle i| \otimes |j\rangle\langle j|,$$

avec $\lambda_{ij} \geqslant 0, \forall i,j$. Comme U est indépendante du choix des bases, son expression reste valable dans cette base où C est diagonale. On a donc :

$$\begin{aligned}
\mathrm{Tr}(UC) &= \sum_{i,j,k,l} \lambda_{kl} \mathrm{Tr}\big(|i\rangle\langle j|k\rangle\langle k| \otimes |j\rangle\langle i|l\rangle\langle l|\big) \\
&= \sum_{i,j,k,l} \lambda_{kl} \delta_{jk}\delta_{il} \mathrm{Tr}\big(|i\rangle\langle k|\big) \mathrm{Tr}\big(|j\rangle\langle l|\big) \\
&= \sum_{i,j,k,l} \lambda_{kj} \delta_{jk}\delta_{il}\delta_{ik}\delta_{jl} \\
&= \sum_{i} \lambda_{ii} \geqslant 0.
\end{aligned}$$

□

Lemme 11. *Soit* $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_1), \mathcal{L}(H_2)\big)$. *Alors* Λ *est positive si et seulement si* $\Lambda^* \in \mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$ *est aussi positive.*

Démonstration. Ceci est simple à démontrer. Remarquons d'abord qu'il suffit de montrer un seul sens. Tout opérateur positif étant somme à coefficients positifs de projecteurs, il suffit de montrer que pour tous projecteurs P_1 sur H_1 et P_2 sur H_2, on a $\mathrm{Tr}\big(\Lambda^*(P_2)P_1\big) \geqslant 0$.

$$\mathrm{Tr}\big(\Lambda^*(P_2)P_1\big) = \langle P_1, \Lambda^*(P_2)\rangle = \langle \Lambda(P_1), P_2\rangle = \overline{\mathrm{Tr}\big(\Lambda(P_1)P_2\big)} \geqslant 0$$

□

On a ici utilisé l'hermiticité du produit scalaire et le caractère autoadjoint du projecteur P_2.

Tout ceci permet d'arriver au théorème suivant :

Théorème 12. *Un état* ϱ *sur* $H_1 \otimes H_2$ *est séparable si et seulement si, pour toute application positive* $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$, *l'opérateur* $(I \otimes \Lambda)\varrho$ *est un opérateur positif sur* $H_1 \otimes H_1$.

Démonstration. On considère toujours $\mathcal{E}_s(H)$ comme l'enveloppe convexe fermée de l'ensemble des états de la forme (1) : $\sum_{i,j} \lambda_{ij} \varrho_{i1} \otimes \varrho_{j2}$.

Soit $\varrho \in \mathcal{E}_s(H)$. Il existe une suite $(\varrho_n)_{n\in\mathbb{N}}$ d'états de la forme (1) tels que $\varrho_n \longrightarrow \varrho$ en norme. $\forall n \in \mathbb{N}, (\mathbb{I} \otimes \Lambda)\varrho_n \in \mathcal{H}^+(H_1 \otimes H_1)$, car pour tous états

ϱ_1 et ϱ_2 sur H_1 et H_2, on a $(\mathbb{I} \otimes \Lambda)(\varrho_1 \otimes \varrho_2) = \varrho_1 \otimes \Lambda(\varrho_2)$ qui est toujours un produit tensoriel d'opérateurs positifs, donc positif sur $H_1 \otimes H_1$.

Ensuite, comme Λ est linéaire continue, $(\mathbb{I} \otimes \Lambda) : H_1 \otimes H_2 \longrightarrow H_1 \otimes H_1$ est linéaire continue, ce qui équivaut à dire que $||(\mathbb{I} \otimes \Lambda)|| < \infty$. Donc $||(\mathbb{I} \otimes \Lambda)\varrho_n - (\mathbb{I} \otimes \Lambda)\varrho|| \leqslant ||(\mathbb{I} \otimes \Lambda)||\,||\varrho_n - \varrho||$ et donc $(\mathbb{I} \otimes \Lambda)\varrho_n \longrightarrow (\mathbb{I} \otimes \Lambda)\varrho$ en norme. Pour conclure, il suffit de remarquer que $\mathcal{H}^+(H_1 \otimes H_1)$ est un fermé de $\mathcal{L}(H_1 \otimes H_1)$, et on a donc que $(\mathbb{I} \otimes \Lambda)\varrho$ est un opérateur positif.

Réciproquement, supposons que $(\mathbb{I} \otimes \Lambda)\varrho$ est positif sur $H_1 \otimes H_1$ pour toute application positive $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$. Alors d'après le lemme 10, on a, pour toute application Λ,

$$\mathrm{Tr}\big(U(\mathbb{I} \otimes \Lambda)\varrho\big) \geqslant 0.$$

Or cette quantité vaut

$$\begin{aligned} \mathrm{Tr}\big(U(\mathbb{I} \otimes \Lambda)\varrho\big) &= \langle U, (\mathbb{I} \otimes \Lambda)\varrho\rangle \\ &= \langle (\mathbb{I} \otimes \Lambda^*)U, \varrho\rangle \\ &= \overline{\mathrm{Tr}\big((\mathbb{I} \otimes \Lambda^*)U\varrho\big)} \\ &= \overline{\mathrm{Tr}\big(S(\Lambda^*)\varrho\big)} \end{aligned}$$

Donc $\mathrm{Tr}\big(S(\Lambda^*)\varrho\big) \geqslant 0$ pour toute application positive $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$. D'après la proposition 7 et le lemme 11, on a la séparabilité de ϱ. □

Ceci a en particulier pour conséquence l'existence d'états intriqués. En effet, revenons sur l'état P_+ que nous avons examiné dans la section 3.2. Nous avons alors vu que $(\mathbb{I} \otimes T)P_+$ n'est pas positive. Donc P_+ est un état intriqué d'après le critère d'intrication que nous venons d'établir.

3.5 Le critère PPT

D'après la proposition 3, pour un état intriqué ϱ donné, il existe un opérateur $A \in \mathcal{L}(H_1 \otimes H_2)$ qui satisfait

$$\forall \sigma \in \mathcal{E}_s(H)\ \mathrm{Tr}(A\sigma) \geqslant 0 \text{ et } \mathrm{Tr}(A\varrho) < 0.$$

A est appelé un **témoin** d'intrication. L'isomorphisme S introduit dans la proposition 6 permet d'établir une bijection entre les témoins d'intrication et les applications positives non complètement positives (bien entendu, ces dernières n'ont aucune contribution dans le critère de Horodecki, puisque $(\mathbb{I} \otimes \Lambda)$ est forcément positive si Λ est complètement positive). Réciproquement, l'image d'une application positive non complètement positive par S peut aussi être le témoin d'une famille d'états intriqués. En choisissant bien le témoin, on peut développer une série de conditions nécéssaires de séparabilité. On en cite une : le critère de la transposition partielle positive, qui possède un intérêt particulier qu'on explicitera dans la suite.

Proposition 13. *On désigne par T la transposition sur $\mathcal{L}(H_2)$, et $\mathbb{I}$ l'identité sur $\mathcal{L}(H_1)$. On définit la transposition partielle T_2 par :*

$$T_2 := \mathbb{I} \otimes T.$$

Si $\varrho \in \mathcal{E}(H_1 \otimes H_2)$ est séparable, alors $T_2(\varrho)$ est un opérateur positif dans $\mathcal{E}(H_1 \otimes H_2)$.

Cette condition nécéssaire est appelée **le critère de la transposition partielle positive**, ou **PPT** (positive partial transposition).

Démonstration. Un état séparable $\varrho \in \mathcal{L}(H_1 \otimes H_2)$ s'écrit comme $\sum_{i,j} p_{ij} \varrho_i^1 \otimes \varrho_j^2$, avec $\sum_{i,j} p_{ij} = 1$ et $\varrho_i^1 \in \mathcal{E}(H_1), \varrho_j^2 \in \mathcal{E}(H_2), \forall i, j$. Ainsi les $T(\varrho_j^2)$ sont des opérateurs positifs dans $\mathcal{L}(H_2)$, car la transposition est une application positive, donc les $\varrho_i^1 \otimes T(\varrho_j^2)$ sont également positifs. Or, on a :

$$T_2(\varrho) = \sum_{i,j} p_{ij} \varrho_i^1 \otimes T(\varrho_j^2),$$

et la somme d'opérateurs positifs est encore positive. □

Par rapport au critère de Horodecki qui n'est pas constructif car la famille des applications positives est longue à décrire, le critère PPT a l'avantage d'être simple et rapide. Le seul défaut est qu'il ne s'agit pas d'une condition suffisante. Néanmoins, les résultats suivants nous aideront à palier en partie ce manque.

Définition 5. *Une application positive $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$ est dite **décomposable** si elle peut se mettre sous la forme*

$$\Lambda = \Lambda_{CP}^1 + \Lambda_{CP}^2 \circ T,$$

avec Λ_{CP}^1 et Λ_{CP}^2 des applications complètement positives dans $\mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$ et T la transposition.

On admet le théorème suivant[3] :

Théorème 14. *En faibles dimensions,* i.e. $\dim(H_1) = 2$, $\dim(H_2) = 2$ *ou* 3, *toute application positive est décomposable.*

Ce théorème nous aidera à montrer la proposition suivante :

Proposition 15. *En faibles dimensions (définies ci-dessus), le critère PPT est une condition nécéssaire et suffisante de séparabilité.*

Démonstration. Il suffit de montrer que c'est une condition suffisante.
Soit $\varrho \in \mathcal{E}(H_1 \otimes H_2)$. Supposons que $T_2(\varrho)$ est un opérateur positif. Soit $\Lambda \in \mathcal{L}\big(\mathcal{L}(H_2), \mathcal{L}(H_1)\big)$ une application positive. Comme on est en faibles dimensions, le théorème 14 permet de décomposer Λ en $\Lambda^1_{CP} + \Lambda^2_{CP} \circ T$. Ainsi pour un opérateur positif $\varrho \in \mathcal{H}^+(H_1 \otimes H_2)$, on a

$$(\mathbb{I} \otimes \Lambda)\varrho = ((\mathbb{I} \otimes \Lambda^1_{CP})\varrho + (\mathbb{I} \otimes \Lambda^2_{CP})T_2(\varrho).$$

Or, Λ^1_{CP} et Λ^2_{CP} sont complètement positives donc $\mathbb{I} \otimes \Lambda^1_{CP}$ et $\mathbb{I} \otimes \Lambda^2_{CP}$ sont positives ; de plus, ϱ et $T_2(\varrho)$ sont supposés positifs, donc $(\mathbb{I} \otimes \Lambda)\varrho$ aussi. Ceci est vrai pour toute application positive Λ, donc d'après la proposition 12, ϱ est séparable. $\square$

Malheureusement, en dimensions plus élevées, il existe des applications positives non décomposables. Le critère PPT n'est donc plus suffisant pour juger la séparabilité. La classe des états intriqués qui satisfont quand même le critère PPT porte le nom d'**intrication liée** (*bound entenglement*), en opposition avec l'**intrication libre** (*free entenglement*). Ce sont des états faiblement intriqués qui sont difficilement utilisables dans la communication quantique.

4 Généralisation en dimension infinie

Si les espaces de Hilbert ne sont plus de dimension finie, alors la généralisation des résultats précédents est délicate. Nous présentons ici schématiquement les outils nécessaires à l'étude en dimension infinie, sans revenir sur l'ensemble des propositions et théorèmes énoncés dans le texte.

On se place dans un espace de Hilbert séparable H. Notons $|e_i\rangle_{i\in\mathbb{N}}$ une base hilbertienne de H. La trace n'est plus définie dans H tout entier, car d'après la définition usuelle de la trace en dimension finie, la trace de l'identité dans H serait infinie.

Néanmoins, comme pour un opérateur positif A, on a que $\forall i \in \mathbb{N}$, $\langle Ae_i|e_i\rangle \geqslant 0$, on définit alors la trace sur $\mathcal{H}^+(H)$ par :

$$\mathrm{Tr}(A) := \sum_i \langle Ae_i|e_i\rangle,$$

la trace étant à valeur dans $[0, \infty]$. Grâce à la trace définie sur $\mathcal{H}^+(H)$, on peut définir la classe des **opérateurs à trace** par :

$$\mathcal{J}_1 := \left\{A \in \mathcal{L}(H) | \ \mathrm{Tr}\big((A^*A)^{1/2}\big) < \infty\right\},$$

puisque $(A^*A)^{1/2}$ est un opérateur positif. De plus, la trace est bien définie sur $\mathcal{J}_1$, car on peut montrer que $\mathrm{Tr}(A) = \sum_i \langle Ae_i|e_i\rangle$ est une somme absolument convergente.

Définissons maintenant un autre sous-espace de $\mathcal{L}(H)$: l'espace des **opérateurs de Hilbert-Schmidt**.

$$\mathcal{J}_2 := \left\{A \in \mathcal{L}(H) | \ \mathrm{Tr}\big((A^*A)\big) < \infty\right\}$$

On vérifie que $||A||_{\mathrm{Tr}} = \sqrt{\mathrm{Tr}(A^*A)}$ est une norme et $\langle A, B\rangle_{\mathrm{Tr}}$ un produit scalaire. En effet, pour $A = (\lambda_{ij})$ dans $\mathcal{L}(H)$, on a :

$$||A||_{\mathrm{Tr}} = \sqrt{\mathrm{Tr}(A^*A)} = \sqrt{\sum_{i,j} \lambda_{ij}^2}$$

Il est alors possible d'en déduire que $\big(\mathcal{J}_2, || \cdot ||_{\mathrm{Tr}}\big)$ est isomorphe à $\big(l^2(\mathbb{N}^2), ||\cdot||_2\big)$, et est donc bien un espace de Hilbert. Ensuite, pour généraliser les théorèmes et les propositions en dimension infinie, on se propose de restreindre $\mathcal{L}(H)$ à $\mathcal{J}_2(H)$.

Remarquons que $\mathcal{E}(H) \subset \mathcal{J}_2(H)$. En effet, $\mathcal{E}(H) \subset \mathcal{H}^+(H)$, donc pour un état $\varrho \in \mathcal{E}(H), \mathrm{Tr}\big((\varrho^*\varrho)^{1/2}\big) = \mathrm{Tr}(\varrho) = 1 < \infty$, et donc $\mathcal{E}(H) \subset \mathcal{J}_1(H)$.

Or $\mathcal{J}_1(H) \subset \mathcal{J}_2(H)$, donc $A \in \mathcal{J}_2(H)$. On a donc $\mathcal{E}(H) \subset \mathcal{J}_2(H)$. Partant de là, pour donner un ordre d'idées, la proposition 3 par exemple resterait valable en travaillant dans $\mathcal{J}_2(H)$, puisque dans cet espace de Hilbert, on aurait encore à notre disposition le théorème d'Hahn-Banach. Il faudrait traiter ainsi chaque proposition et vérifier la cohérence de chaque définition, en particulier en ce qui concerne la continuité des applications introduites, (comme l'isomorphisme S par exemple), et la décomposition des opérateurs sur une base hilbertienne.

5 Conclusion

Depuis la naissance de la Mécanique Quantique, la notion d'intrication joue un rôle privilégié : tandis que les physiciens de l'école de Copenhague cherchaient déjà à l'étudier, les partisants de la Physique Classique tentaient de démontrer son absurdité. Après des années d'ardents débats, quand les inégalités de Bell permettent de démontrer pour la première fois l'existence d'états intriqués, elles donnent aussi le premier critère de séparabilité, car elles doivent être vérifiées par tout état séparable. La famille d'inégalités de Bell développées au cours du temps donne donc une série de conditions nécessaires de séparabilité. Malheureusement, ce sont des critères faibles : il existe une large classe d'états intriqués qui satisfont toute inégalité standard de Bell.

L'introduction du critère PPT par *A. Peres* ouvre une voie nouvelle à notre problème. En effet, bien qu'il s'agisse encore d'une condition non suffisante, c'est le premier critère *structurel* : au lieu de donner quelques conditions ou inégalités que les états séparables doivent satisfaire, le critère PPT donne plutôt une prédiction sur le comportement des états séparables suite à une opération quantique, qui est ici la transposition partielle.

Ce nouveau critère a aussi fait remarquer le lien étroit entre la recherche des critères de séparabilité et la théorie des applications positives, car la transposition partielle est un exemple simple d'application positive non complètement positive. La recherche interdisciplinaire s'avère fructueuse : le critère de Horodecki, qui est au sein de notre exposé, en est un résultat important. Par ailleurs, la traduction physique des applications positives assure l'aspect pratique du critère de Horodecki.

Remarquons enfin que malgré l'apparente simplicité du problème, (la définition des états séparables n'utilise aucune notion compliquée), la caractérisation des états intriqués est loin d'être évidente, et n'est à ce jour que partiellement résolue dans le cas général. On a pu voir que les preuves n'utilisent, du moins en dimension finie, que des outils élémentaires, et malgré cela, l'intrication ne se laisse pas entièrement dévoiler.

Remerciements

Nous tenons à remercier notre encadrant Thierry Paul qui a su nous guider dans ce domaine à l'interface entre la physique et les mathématiques.

Références

[1] M, P. and R. Horodecki, *Mixed-state entanglement and quantum communication*, in "Quantum Information : An Introduction to Basic Theoretical Concepts and Experiments", "Springer Tracts in Modern Physics", 2001 et arXiv : quant-ph/0109124.

[2] T. Levy http ://www.dma.ens.fr/edition/NotesGDT/GTcalcul_quantique/index.html

[3] S. L. Woronowicz : Rep. Math. Phys. 10, 165 (1976).

[4] M. Reed, B. Simon, Methods of modern mathematical physics, I : Functional Analysis, pp. 210-213