UNIVERSITÉ D'AIX-MARSEILLE

RAPPORT DE STAGE

Incompatibilité des mesures quantiques

Antoine ROUX
M2 FunPhys 2018-2019

Tuteur : Ion NECHITA

mars 2019 — juin 2019

1 Introduction

1.1 notations

Soit $\mathcal{X}$ un espace de Hilbert de dimension finie (que l'on abrège en espace euclidien complexe), on définis les ensembles suivants:

$L(\mathcal{X};\mathcal{Y})$ est l'ensemble des opérateurs de $\mathcal{X}$ dans $\mathcal{Y}$
$\mathrm{Pos}(\mathcal{X})$ est l'ensemble des opérateurs positifs semi-définis $\in L(\mathcal{X};\mathcal{X}) = L(\mathcal{X})$, plus précisément:

$$A \in \mathrm{Pos}(\mathcal{X}) \iff \forall x \in \mathcal{X} : x^\star A x \geq 0$$

$\mathrm{Pd}(\mathcal{X})$ est l'ensemble des opérateurs positifs définis:

$$A \in \mathrm{Pd}(\mathcal{X}) \iff \forall x \in \mathcal{X} : x^\star A x > 0$$

$D(\mathcal{X})$ est l'ensemble des opérateurs densités:

$$A \in D(\mathcal{X}) \iff A \in \mathrm{Pos}(\mathcal{X}) \text{ et } \mathrm{Tr}\, A = 1$$

$\mathrm{Herm}(\mathcal{X})$ est l'ensemble des opérateurs hermitiens, $\mathrm{Pos}(\mathcal{X}) \subset \mathrm{Herm}(\mathcal{X})$
$U(\mathcal{X};\mathcal{Y})$ est l'ensemble des isométries de $\mathcal{X}$ dans $\mathcal{Y}$:

$$A \in U(\mathcal{X};\mathcal{Y}) \iff U^\star U = \mathrm{Id}$$

pour $A, B \in L(\mathcal{X};\mathcal{Y})$:
$\langle A, B\rangle$ est le produit scalaire de Hilbert-Schmidt:

$$\langle A, B\rangle = \mathrm{Tr}\, A^\star B$$

à ce produit scalaire est associé la 2-norme:

$$||A||_2 = \sqrt{\mathrm{Tr}\,[A^\star A]}$$

introduction Dans ce rapport, nous allons traiter de la notion d'incompatibilité, de son lien avec le concept de guidage, enfin, nous détaillerons un critère d'incompatibilité.
Le domaine de l'information quantique cherche à exploiter les propriétés quantiques de la matière dans le but de calculer et de communiquer. pour cela, il faut traiter avec un maximum de généralité les opérations autorisées. Ces opérations sont effectuées sur des registres.
Un registre est l'abstraction d'un système physique, support de l'information. A chaque registre est attaché un espace vectoriel complexe (de dimension finie), muni d'un produit scalaire hermitien (espace complexe euclidien) c'est l'espace du registre.
L'état d'un registre X est un opérateur densité $\rho \in D(\mathcal{X})$, où $\mathcal{X}$ est l'espace du registre.

1.2 Opérations élémentaires

les opérations élémentaires sur les registres sont les suivantes:
1) couplage :
Si X_1 et X_2 sont deux registres d'espace $\mathcal{X}_1$ et $\mathcal{X}_2$, on forme un nouveau registre (X_1, X_2) d'espace $\mathcal{X}_1 \otimes \mathcal{X}_2$
Si avant le couplage $\rho \in D(\mathcal{X}_1)$ et $\sigma \in D(\mathcal{X}_2)$ sont les états respectifs de X_1 et X_2; après le couplage, l'état de (X_1, X_2) est $\rho \otimes \sigma \in D(\mathcal{X}_1 \otimes \mathcal{X}_2)$
2) évolution :
On transforme l'état du registre par une application unitaire $U \in U(\mathcal{X})$: si $\rho \in D(\mathcal{X})$ est l'état avant l'évolution, après celle ci, l'état devient: $U\rho U^\star$.
3) réjection :
Cela consiste à ignorer un registre, ou dit autrement, à le considérer comme dorénavant inaccessible (cela permet de modéliser la perte d'information dans un environnement auquel on n'a pas accès, [9] page 116)
Si $\rho \in D(\mathcal{X}_1 \otimes \mathcal{X}_2)$ est l'état avant la réjection de X_2, après celle ci, l'état devient $\mathrm{Tr}_{\mathcal{X}_2}(\rho)$
Où $\forall(\alpha, \beta) \in L(\mathcal{X}_1) \times L(\mathcal{X}_2)$, $\mathrm{Tr}_{\mathcal{X}_2}(\alpha \otimes \beta) = \alpha \,\mathrm{Tr}(\beta)$ est étendu par bilinéarité à tout $L(\mathcal{X}_1 \otimes \mathcal{X}_2)$.
4) mesure :
Si $A \in \mathrm{Herm}(\mathcal{X})$ est une observable, et si l'état du registre est $\rho \in D(\mathcal{X})$; la probabilité d'obtenir a valeur propre de A est égale à: $p(a) = \mathrm{Tr}(\rho\Pi_a) = \langle \rho, \Pi_a \rangle$ où Π_a est le projecteur orthogonal sur l'espace propre de valeur propre a pour A.

1.3 mesure généralisée

On aura besoin par la suite de traiter plus généralement du concept de mesure; pour cela, introduisons le formalisme des POVM (Positive Operator Valued Measure)
Un POVM est une famille $(P_i)_{1 \leq i \leq n}$ d'opérateurs positifs (i.e. hermitiens et avec toutes leurs valeurs propres ≥ 0) telle que:

$$\sum_{1 \leq i \leq n} P_i = \mathrm{Id}$$

Le résultat i est obtenu avec la probabilité $\mathrm{Tr}\, P_i\rho =< P_i, \rho >$.
De plus, l'état du registre après avoir obtenu le résultat i est égal à :

$$\frac{P_i^{1/2}\rho P_i^{1/2}}{\langle P_i, \rho \rangle}$$

Bien entendu, le concept de POVM est équivalent à celui plus familier d'observable, en fait, on peut montrer que tout POVM peut s'obtenir en combinant les points 1), 2), 3) ci-dessus. plus précisément, on couple le registre X que l'on veut mesurer avec un autre registre Y tel que: $\dim(\mathcal{Y}) = n$ (la taille du POVM), on applique une évolution unitaire au registre (X, Y); enfin, on effectue une mesure

projective sur le registre Y. (pour plus de détail, cf [3] page 94, ainsi que [9] page 110)

1.4 Canaux quantiques

La notion de canal permet de capturer toutes les opérations que l'on peut effectuer sur un registre.
Par définition, un canal du registre X vers le registre Y est une application linéaire $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$ telle que:
a)Φ préserve la trace, i.e.

$$\forall A \in L(\mathcal{X}), \mathrm{Tr}(\Phi(A)) = \mathrm{Tr}(A)$$

b)Φ est complètement positive.
i.e. pour tout espace euclidien complexe $\mathcal{Z}$ et pour tout opérateur positif $A \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Z})$, on a que: $(\Phi \otimes \mathrm{Id}_{\mathcal{Z}})(A) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$

1.5 Représentation de Stinespring

Propriété 1. *Soit $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$ une application linéaire. Φ est un canal ssi il existe il existe un espace euclidien complexe $\mathcal{Z}$ et une isométrie $A \in U(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ tels que:*

$$\forall X \in L(\mathcal{X}) : \Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(AXA^{\star})$$

Pour une démonstration, cf [8] corollaire 2.27
Cette propriété implique que tout canal peut s'obtenir en combinant les opérations élémentaires de couplage (avec le registre Z), d'évolution unitaire (A) et de réjection (du registre Z)

2 Incompatibilité

2.1 incompatibilité des mesures :

Deux POVM $(A_i)_{1 \leq i \leq m}$ et $(B_j)_{1 \leq j \leq n}$ sont dit compatibles s'il existe un POVM $(C_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$ tel que:

$$\forall j : \sum_{1 \leq i \leq m} C_{i,j} = B_j$$

$$\forall i : \sum_{i \leq j \leq n} C_{i,j} = A_i$$

Par définition, deux POVM qui ne sont pas compatibles sont incompatibles. voir [10]

Une définition équivalente de la compatibilité est la suivante:
Soit $\{\mu_{a,x}\}_{1\leq a\leq n}$ et $_{1\leq x\leq m} \in \mathrm{Pos}(\mathcal{X})$, tel que:

$$\forall x \in \{1,...,m\} : \sum_{1\leq a\leq n} \mu_{a,x} = \mathrm{Id}$$

(c'est une famille de POVM paramétrée par x) Cette famille de POVM est compatible ssi il existe un POVM $\{B_\lambda\}_{1\leq\lambda\leq L}$ et une loi de probabilité $p(a|x,\lambda)$ tels que:
$\forall (a,x) \in \{1,...,n\} \times \{1,...,m\}$:

$$\mu(a,x) = \sum_{1\leq\lambda\leq L} p(a|x,\lambda) B_\lambda$$

2.1.1 exemple de mesures incompatibles :

En dimension $d = 2$, un exemple simple de POVM incompatibles est le suivant:
On pose $A_1 = |0\rangle\langle 0|$, $A_2 = |1\rangle\langle 1|$
Ainsi que: $B_1 = |+\rangle\langle +|$, $B_2 = |-\rangle\langle -|$
avec: $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$
On cherche $C_{1,1}, C_{1,2}, C_{2,1}, C_{2,2}$ opérateur positifs tels que:

$$C_{1,1} + C_{1,2} = A_1$$
$$C_{1,1} + C_{2,1} = B_1$$
$$C_{1,1} + C_{1,2} + C_{2,1} + C_{2,2} = \mathrm{Id}$$

La première égalité implique que $\mathrm{Im}\, C_{1,1} \subset \mathrm{Im}\, |0\rangle\langle 0|$ (voir le prochain lemme) et donc que $C_{1,1} = \lambda |0\rangle\langle 0|$ pour un certain $0 \leq \lambda \leq 1$
Or, on doit avoir pour la même raison $C_{1,1} = \mu |+\rangle\langle +|$
$\Rightarrow \mu = \lambda = 0 \Rightarrow C_{1,1} = 0$
Pour la même raison, $C_{1,2} = 0$ et donc: $|0\rangle\langle 0| = C_{1,1} + C_{1,2} = 0$ d'où la contradiction.

Lemme. *Soit A, B et C éléments de $\mathrm{Pos}(\mathcal{X})$ tels que: $A + B = C$, alors:* $\mathrm{Im}\, C = \mathrm{Im}\, A + \mathrm{Im}\, B$

preuve. en effet, en utilisant $\ker A = (\mathrm{Im}\, A)^\perp$ et :

$$\mathrm{Im}\, C = \mathrm{Im}\, A + \mathrm{Im}\, B$$
$$\iff (\mathrm{Im}\, C)^\perp = (\mathrm{Im}\, A + \mathrm{Im}\, B)^\perp$$

or $(V + W)^\perp = V^\perp \cap W^\perp$ donc:

$$\iff \ker C = \ker A \cap \ker B$$

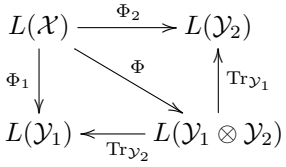
il suffit donc de vérifier cette dernière égalité:

$$x \in \ker C \iff Cx = 0 \iff x^\star Cx = 0$$
$$\iff x^\star Ax + x^\star Bx = 0$$
$$\iff x^\star Ax = x^\star Bx = 0$$
$$\iff Ax = Bx = 0 \iff x \in \ker A \cap \ker B$$

□

2.2 incompatibilité des canaux

Deux canaux $\Phi_1 : L(\mathcal{X}) \to L(\mathcal{Y}_1)$
et $\Phi_2 : L(\mathcal{X}) \to L(\mathcal{Y}_2)$, sont dit compatibles s'il existe un canal $\Phi : L(\mathcal{X}) \to L(\mathcal{Y}_1 \otimes \mathcal{Y}_2)$ rendant le diagramme suivant commutatif:



2.2.1 exemple: le théorème de non-diffusion.

Ce théorème affirme que $\Phi_1 = \Phi_2 = \mathrm{Id}_{L(\mathcal{X})}$ sont incompatibles.
Plus précisément:

Propriété 2. *Soit un canal $\Phi : L(\mathcal{X}) \to L(\mathcal{X} \otimes \mathcal{X})$ et deux états $\rho_1, \rho_2 \in D(\mathcal{X})$ inversibles tels que $\mathrm{Tr}_1(\Phi(\rho_1)) = \mathrm{Tr}_2(\Phi(\rho_1)) = \rho_1$ ainsi que: $\mathrm{Tr}_1(\Phi(\rho_2)) = \mathrm{Tr}_2(\Phi(\rho_2)) = \rho_2$; Alors, $[\rho_1, \rho_2] = 0$*

voir [7]
Nous allons démontrer ce théorème en plusieurs étapes, commençons par introduire la notion de fidélité ainsi que ces propriétés élémentaires.

Fidélité

Propriété 3. *Par définition:*
Pour $\rho_1, \rho_2 \in D(\mathcal{X})$:

$$F(\rho_1, \rho_2) = \mathrm{Tr}\sqrt{\rho_0^{1/2}\rho_1\rho_0^{1/2}}$$

On a les propriétés suivantes (admises, pour les preuves, voir [8] proposition 3.12):

$$F(\rho_0, \rho_1) = 1 \iff \rho_0 = \rho_1$$
$$F(\rho_0, \rho_1) = 0 \iff \mathrm{Im}\,\rho_0 \perp \mathrm{Im}\,\rho_1$$

$$\forall U \in U(\mathcal{X}), F(U\rho_0 U^\star, U\rho_1 U^\star) = F(\rho_0, \rho_1)$$
$$F(\rho_0 \otimes \sigma_0, \rho_1 \otimes \sigma_1) = F(\rho_0, \rho_1) F(\sigma_0, \sigma_1)$$

Propriété 4. $\forall \rho_0, \rho_1 \in D(\mathcal{X})$

$$F(\rho_0, \rho_1) = \min_{\{E_b\} povm} \sum_b \sqrt{\langle \rho_0, E_b \rangle} \sqrt{\langle \rho_1, E_b \rangle}$$

preuve. Pour tout POVM $\{E_b\}$, et pour tout U unitaire:

$$\sum_b \sqrt{\langle \rho_0, E_b \rangle} \sqrt{\langle \rho_1, E_b \rangle}$$
$$= \sum_b \sqrt{\mathrm{Tr}(\rho_0 E_b)} \sqrt{\mathrm{Tr}\,(\rho_1 E_b)}$$
$$= \sum_b \sqrt{\mathrm{Tr}\left[U \rho_0^{1/2} E_b \rho_0^{1/2} U^\star\right]} \sqrt{\mathrm{Tr}\left[\rho_1^{1/2} E_b \rho_1^{1/2}\right]}$$
$$= \sum_b \sqrt{\langle E_b^{1/2} \rho_0^{1/2} U^\star, E_b^{1/2} \rho_0^{1/2} U^\star \rangle} \sqrt{\langle E_b^{1/2} \rho_1^{1/2}, E_b^{1/2} \rho_1^{1/2} \rangle}$$

par Cauchy-Schwarz:

$$\geq \sum_b \left| \langle E_b^{1/2} \rho_0^{1/2} U^\star, E_b^{1/2} \rho_1^{1/2} \rangle \right|$$
$$= \sum_b \left| \mathrm{Tr}\left[U \rho_0^{1/2} E_b^{1/2} E_b^{1/2} \rho_1^{1/2}\right] \right|$$
$$\geq \left| \sum_b \mathrm{Tr}\left[U \rho_0^{1/2} E_b \rho_1^{1/2}\right] \right| = \left| \mathrm{Tr}\left[U \rho_0^{1/2} \rho_1^{1/2}\right] \right|$$

or, il existe U unitaire tel que: $U \rho_0^{1/2} \rho_1^{1/2} = \sqrt{\rho_1^{1/2} \rho_0 \rho_1^{1/2}}$ (cela se voit en écrivant la décomposition en valeurs singulières de $\rho_0^{1/2} \rho_1^{1/2}$ cf [8] théorème 1.6)

$$\Rightarrow \sum_b \sqrt{\langle \rho_0, E_b \rangle} \sqrt{\langle \rho_1, E_b \rangle} \geq \mathrm{Tr} \sqrt{\rho_1^{1/2} \rho_0 \rho_1^{1/2}} = F(\rho_0, \rho_1)$$

Montrons que cette borne est atteinte:
Soit $M = \rho_1^{-1/2} \sqrt{\rho_1^{1/2} \rho_0 \rho_1^{1/2}} \rho_1^{-1/2} > 0$ Considérons la décomposition spectrale de M:

$$M = \sum_b \mu_b |b\rangle\langle b|$$

avec $\forall b : \mu_b > 0$ et $|b\rangle$ base orthonormée.
on défini: $E_b = |b\rangle\langle b|$, on voit que (E_b) est un POVM.

on a: $ME_b^{1/2} = \mu_b E_b^{1/2} (\forall b)$

Soit $U \in U(\mathcal{X})$ tel que: $U\rho_0^{1/2}\rho_1^{1/2} = \sqrt{\rho_1^{1/2}\rho_0\rho_1^{1/2}}$
On a alors:

$$\rho_1^{-1/2} U \rho_0^{1/2} = M$$
$$\Rightarrow \rho_1^{-1/2} U \rho_0^{1/2} E_b^{1/2} = \mu_b E_b^{1/2}$$

donc:

$$U\rho_0^{1/2} E_b^{1/2} = \mu_b \rho_1^{1/2} E_b^{1/2} (\forall b)$$

on a donc la condition d'égalité pour Cauchy-Schwarz,

$$\left\| E_b^{1/2}\rho_0^{1/2} U^\star \right\|_2 \left\| E_b^{1/2}\rho_1^{1/2} \right\|_2 = \left| \langle E_b^{1/2}\rho_0 U^\star, E_b^{1/2}\rho_1^{1/2} \rangle \right| (\forall b)$$

$$\iff \sqrt{\mathrm{Tr}\left[U\rho_0^{1/2} E_b \rho_0^{1/2} U^\star\right]} \sqrt{\mathrm{Tr}\left[\rho_1^{1/2} E_b \rho_1^{1/2}\right]} = \left| \mathrm{Tr}\left[U\rho_0^{1/2} E_b \rho_1^{1/2}\right] \right|$$
$$= \left| \mathrm{Tr}\left[U\rho_0^{1/2} E_b^{1/2} E_b^{1/2} \rho_1^{1/2}\right] \right|$$
$$= \left| \mathrm{Tr}\left[\mu_b \rho_1^{1/2} E_b^{1/2} E_b^{1/2} \rho_1^{1/2}\right] \right|$$
$$= |\mu_b \,\mathrm{Tr}\,[\rho_1 E_b]| = \underbrace{\mu_b}_{>0} \underbrace{\mathrm{Tr}\,[\rho_1 E_b]}_{\geq 0}$$

donc:

$$\sum_b \sqrt{\mathrm{Tr}\,[\rho_0 E_b]} \sqrt{\mathrm{Tr}\,[\rho_1 E_b]} = \sum_b \mathrm{Tr}\,[\rho_1 \mu_b E_b] = \sum_b \mathrm{Tr}\left[U\rho_0^{1/2} E_b \rho_1^{1/2}\right]$$

$$= \mathrm{Tr}\left[U\rho_0^{1/2}\rho_1^{1/2}\right] = \mathrm{Tr}\left[\sqrt{\rho_1^{1/2}\rho_0\rho_1^{1/2}}\right] = F(\rho_0, \rho_1)$$

$\Rightarrow$ on a bien $F(\rho_0, \rho_1) = \min_{(E_b), povm} \sum_b \sqrt{\langle \rho_0, E_b \rangle} \sqrt{\langle \rho_1, E_b \rangle}$
et le minimum est atteint pour $E_b = |b\rangle\langle b|$ avec $|b\rangle$ tel que: $M = \sum_b \mu_b |b\rangle\langle b|$.
□

Inversement, on a le corolaire suivant:

Propriété 5. *Si $U \in U(\mathcal{X})$ est tel que $U\rho_0^{1/2}\rho_1^{1/2} = \sqrt{\rho_1^{1/2}\rho_0\rho_1^{1/2}}$, et si $\{E_b\}$ est optimal pour $\{\rho_0, \rho_1\}$, alors:*

$$\forall b, \exists \mu_b \in \mathbb{C} : U\rho_0^{1/2} E_b^{1/2} = \mu_b \rho_1^{1/2} E_b^{1/2}$$

de plus, les μ_b ont tous la même phase.

Propriété 6. *Soit* $\rho_0, \rho_1 \in D(\mathcal{X})$ *et* $\Phi : L(\mathcal{X}) \to L(\mathcal{X} \otimes \mathcal{X})$ *un canal, tels que:* $\forall s \in \{0,1\} : \mathrm{Tr}_1 [\Phi(\rho_s)] = \mathrm{Tr}_2 [\Phi(\rho_s)] = \rho_s$*, alors:*

$$F(\Phi(\rho_0), \Phi(\rho_1)) = F(\rho_0, \rho_1)$$

preuve. Tout d'abord, on a: $F(\Phi(\rho_0), \Phi(\rho_1)) \leq F(\rho_0, \rho_1)$
en effet, $\mathrm{Tr}[\Phi(\rho_s)(E_b \otimes \mathrm{Id})] = \mathrm{Tr}_1 [\mathrm{Tr}_2 [\Phi(\rho_s)(E_b \otimes \mathrm{Id})]]$

$$= \mathrm{Tr}[E_b \, \mathrm{Tr}_2 [\Phi(\rho_s)]] = \mathrm{Tr}[\rho_s E_b]$$

d'où:

$$F(\rho_0, \rho_1) = \min_{\{E_b\}\mathrm{povm}} \sum_b \sqrt{\langle \rho_0, E_b \rangle} \sqrt{\langle \rho_1, E_b \rangle}$$

$$= \min_{\{E_b\}\mathrm{povm}} \sum_b \sqrt{\langle \Phi(\rho_0), E_b \otimes \mathrm{Id} \rangle} \sqrt{\langle \Phi(\rho_1), E_b \otimes \mathrm{Id} \rangle}$$

$$\geq \min_{\{A_c\}\mathrm{povm}} \sum_c \sqrt{\langle \Phi(\rho_0), A_c \rangle} \sqrt{\langle \Phi(\rho_1), A_c \rangle}$$

$$= F(\Phi(\rho_0), \Phi(\rho_1))$$

d'autre part, si on prend la représentation de Stinespring de $\Phi(X) = \mathrm{Tr}_{\mathcal{Z}} [UXU^\star]$, avec $\mathcal{Z}$ un certain espace euclidien complexe et $U \in U(\mathcal{X}; \mathcal{X} \otimes \mathcal{Z})$ une certaine isométrie:
en répétant la preuve qui viens juste d'être donnée, tout en effectuant les remplacements suivants:
$\rho_0 \to \Phi(\rho_0)$
$\rho_1 \to \Phi(\rho_1)$
$\Phi(\rho_0) \to U\rho_0 U^\star$
$\Phi(\rho_1) \to U\rho_1 U^\star$

on obtient:

$$F(\rho_0, \rho_1) = F(U\rho_0 U^\star, U\rho_1 U^\star) \leq F(\mathrm{Tr}_{\mathcal{Z}} [U\rho_0 U^\star], \mathrm{Tr}_{\mathcal{Z}} [U\rho_1 U^\star])$$

$$= F(\Phi(\rho_0), \Phi(\rho_1))$$

$$\Rightarrow F(\Phi(\rho_0), \Phi(\rho_1)) = F(\rho_0, \rho_1)$$

□

Comme corollaire, on a:

Propriété 7. *Si* $F(\rho_0, \rho_1) = F(\Phi(\rho_0), \Phi(\rho_1))$ *et si* $\{E_b\}$ *est optimal pour* $\{\rho_0, \rho_1\}$*, alors:* $\{E_b \otimes \mathrm{Id}\}$ *et* $\{\mathrm{Id} \otimes E_b\}$ *sont optimaux pour* $\{\Phi(\rho_0), \Phi(\rho_1)\}$

En combinant cela avec la propriété (5), cela donne:

Propriété 8. *Il existe $\widetilde{U}$ et $\widetilde{V}$ unitaires tels que:*

$$\widetilde{U}\Phi(\rho_0)^{1/2}\Phi(\rho_1)^{1/2} = \widetilde{V}\Phi(\rho_0)^{1/2}\Phi(\rho_1)^{1/2} = \sqrt{\Phi(\rho_1)^{1/2}\Phi(\rho_0)\Phi(\rho_1)^{1/2}}$$

et, $\forall b$:

$$\widetilde{U}\Phi(\rho_0)^{1/2}(\mathrm{Id}\otimes E_b) = \alpha_b\Phi(\rho_1)^{1/2}(\mathrm{Id}\otimes E_b)$$

$$\widetilde{V}\Phi(\rho_0)^{1/2}(E_b\otimes \mathrm{Id}) = \beta_b\Phi(\rho_1)^{1/2}(E_b\otimes \mathrm{Id})$$

$$\alpha_b, \beta_b \geq 0$$

Sachant cela, on défini $G = \sum_b \alpha_b|b\rangle\langle b|$ et $H = \sum_b \beta_b|b\rangle\langle b|$:
Par construction: $G, H \geq 0$

Propriété 9. $G = H = M$

preuve. En sommant les deux dernières égalités de (8):

$$\begin{cases} \widetilde{U}\Phi(\rho_0)^{1/2} = \Phi(\rho_1)^{1/2}\,(\mathrm{Id}\otimes G) \\ \widetilde{V}\Phi(\rho_0)^{1/2} = \Phi(\rho_1)^{1/2}\,(H\otimes \mathrm{Id}) \end{cases} \tag{1}$$

ce qui donne:

$$\begin{cases} \Phi(\rho_0) = \Phi(\rho_0)^{1/2}\widetilde{U}^{\star}\Phi(\rho_1)^{1/2}\,(\mathrm{Id}\otimes G) \\ \Phi(\rho_0) = \Phi(\rho_0)^{1/2}\widetilde{V}^{\star}\Phi(\rho_1)^{1/2}\,(H\otimes \mathrm{Id}) \end{cases}$$

on prend la première trace partielle pour la première équation, et la seconde trace partielle pour la seconde équation:

$$\begin{cases} \rho_0 = \mathrm{Tr}_1\left[\Phi(\rho_0)^{1/2}\widetilde{U}^{\star}\Phi(\rho_1)^{1/2}\right]G \\ \rho_0 = \mathrm{Tr}_2\left[\Phi(\rho_0)^{1/2}\widetilde{V}^{\star}\Phi(\rho_1)^{1/2}\right]H \end{cases} \tag{2}$$

on transforme le système (1) en:

$$\begin{cases} \Phi(\rho_1)^{1/2}\widetilde{U}\Phi(\rho_0)^{1/2} = \Phi(\rho_1)\,(\mathrm{Id}\otimes G) \\ \Phi(\rho_1)^{1/2}\widetilde{V}\Phi(\rho_0)^{1/2} = \Phi(\rho_1)\,(H\otimes \mathrm{Id}) \end{cases}$$

puis on prend la première trace partielle pour la première équation, et la seconde trace partielle pour la seconde équation:

$$\begin{cases} \mathrm{Tr}_1\left[\Phi(\rho_1)^{1/2}\widetilde{U}\Phi(\rho_0)^{1/2}\right] = \rho_1 G \\ \mathrm{Tr}_2\left[\Phi(\rho_1)^{1/2}\widetilde{V}\Phi(\rho_0)^{1/2}\right] = \rho_1 H \end{cases}$$

$$\Longleftrightarrow$$

$$\left\{ \begin{array}{l} \mathrm{Tr}_1 \left[\Phi(\rho_0)^{1/2} \widetilde{U}^\star \Phi(\rho_1)^{1/2} \right] = G\rho_1 \\ \mathrm{Tr}_2 \left[\Phi(\rho_0)^{1/2} \widetilde{V}^\star \Phi(\rho_1)^{1/2} \right] = H\rho_1 \end{array} \right. \tag{3}$$

Parconséquent, en combinant (2) et (3):

$$\rho_0 = G\rho_1 G = H\rho_1 H$$

par ailleurs, on a les égalités:

$$\left\{ \begin{array}{l} \rho_1^{1/2} \rho_0 \rho_1^{1/2} = \rho_1^{1/2} G \rho_1 G \rho_1^{1/2} = \left(\rho_1^{1/2} G \rho_1^{1/2} \right)^2 \\ \rho_1^{1/2} \rho_0 \rho_1^{1/2} = \rho_1^{1/2} H \rho_1 H \rho_1^{1/2} = \left(\rho_1^{1/2} H \rho_1^{1/2} \right)^2 \end{array} \right.$$

$$\Rightarrow$$

$$\left\{ \begin{array}{l} \rho_1^{1/2} G \rho_1^{1/2} = \sqrt{\rho_1^{1/2} \rho_0 \rho_1^{1/2}} \\ \rho_1^{1/2} H \rho_1^{1/2} = \sqrt{\rho_1^{1/2} \rho_0 \rho_1^{1/2}} \end{array} \right.$$

donc: $G = H = M$ car ρ_0 et ρ_1 sont inversibles

□

On a ainsi:

$$\widetilde{U} \Phi(\rho_0)^{1/2} = \Phi(\rho_1)^{1/2} \left(\mathrm{Id} \otimes M \right)$$

et

$$\widetilde{V} \Phi(\rho_0)^{1/2} = \Phi(\rho_1)^{1/2} \left(M \otimes \mathrm{Id} \right)$$

Propriété 10. *Soit $M = \sum_b \mu_b |b\rangle\langle b|$ la décomposition spectrale de M, avec $\forall b : \mu_b > 0$ et $|b\rangle$ base orthonormée.*
$\forall b, c$ si $\mu_b \neq \mu_c$, alors: $\Phi(\rho_0)^{1/2} |b\rangle |c\rangle = 0$

preuve. En effet:

$$\begin{aligned} \widetilde{V} \Phi(\rho_0)^{1/2} &= \Phi(\rho_1)^{1/2} \left(M \otimes \mathrm{Id} \right) \\ \Rightarrow \Phi(\rho_0)^{1/2} &= \widetilde{V}^\star \Phi(\rho_1)^{1/2} \left(M \otimes \mathrm{Id} \right) \\ \Rightarrow \widetilde{V}^\star \Phi(\rho_1)^{1/2} &= \Phi(\rho_0)^{1/2} \left(M^{-1} \otimes \mathrm{Id} \right) \end{aligned}$$

et donc:

$$\widetilde{V}^\star \widetilde{U} \Phi(\rho_0)^{1/2} = \widetilde{V}^\star \Phi(\rho_1)^{1/2} \left(\mathrm{Id} \otimes M \right) = \Phi(\rho_0)^{1/2} \left(M^{-1} \otimes \mathrm{Id} \right) \left(\mathrm{Id} \otimes M \right)$$

i.e.

$$\widetilde{V}^\star \widetilde{U} \Phi(\rho_0)^{1/2} = \phi(\rho_0)^{1/2} \left(M^{-1} \otimes M \right)$$

ainsi, $\Phi(\rho_0)^{1/2}|b\rangle \otimes |c\rangle$ est vecteur propre de $\widetilde{V}^\star \widetilde{U}$ unitaire, de valeur propre $\frac{\mu_c}{\mu_b} > 0$. Or les valeurs propres d'un opérateur unitaire sont de module 1
$\Rightarrow$ si $\mu_c \neq \mu_b$, alors $\Phi(\rho_0)^{1/2}|b\rangle \otimes |c\rangle = 0$

□

Propriété 11. $M\rho_0 = \rho_0 M$

preuve. $\forall b, b'$:

$$\begin{aligned}\langle b'| \left(M\rho_0 - \rho_0 M\right) |b\rangle &= \left(\mu_{b'} - \mu_b\right) \langle b'|\rho_0|b\rangle \\ &= \left(\mu_{b'} - \mu_b\right) \sum_c \left(\langle b'| \otimes \langle c|\right) \Phi(\rho_0) \left(|b\rangle \otimes |c\rangle\right) \\ = \left(\mu_{b'} - \mu_b\right) \sum_c \Big(\langle b'| \otimes \langle c|\Phi(\rho_0)^{1/2}\Big) \Big(\Phi(\rho_0)^{1/2}|b\rangle \otimes |c\rangle\Big)\end{aligned}$$

deux cas s'offrent à nous:

1)$\mu_{b'} = \mu_b$

$$\Rightarrow \langle b'| \left(M\rho_0 - \rho_0 M\right) |b\rangle = 0$$

2)$\mu_{b'} \neq \mu_b$

$$\Rightarrow \forall c \left[\mu_b \neq \mu_c \vee \mu_{b'} \neq \mu_c\right]$$

$$\Rightarrow \langle b'| \left(M\rho_0 - \rho_0 M\right) |b\rangle = 0$$

donc: $M\rho_0 = \rho_0 M$

□

Propriété 12. $\rho_0\rho_1 = \rho_1\rho_0$

preuve. puisque $\rho_0 = M\rho_1 M$:

$$\rho_0\rho_1 = \rho_0 M^{-1}\rho_0 M^{-1} = M^{-1}\rho_0 M^{-1}\rho_0 = \rho_1\rho_0$$

□

Ceci termine la démonstration du théorème de non-diffusion.

3 Guidage (steering)

3.1 guidage de Schrödinger

Le terme guidage à été introduit par Schrödinger, cela résulte de l'observation que lorsque A (Alice, registre X) et B (Bob, registre Y) partagent un état pur $\Psi \in \mathcal{X} \otimes \mathcal{Y}$, Alice peut, en effectuant une mesure qu'elle effectue sur son registre guider l'état de Bob dans un ensemble d'états possibles après la mesure, cet ensemble dépendant de la mesure (Alice guide ainsi l'état de Bob par le choix de cette mesure.)

exemple: (Voir [6] page 72)
On suppose $\mathcal{X} = \mathcal{Y}$ et $\dim \mathcal{X} = d$
Soit $\{e_i\}_{1 \leq i \leq d}$ une base orthonormée de $\mathcal{X}$, et $\{f_i\}_{1 \leq i \leq d}$ une base orthonormée de $\mathcal{Y}$
Posons

$$\Psi = \sum_{1 \leq i \leq d} e_i \otimes f_i$$

C'est l'état maximalement intriqué

Soit maintenant $\{\bar{f}_i\}_{1 \leq i \leq d}$ un autre base orthonormée de $\mathcal{Y}$, et $U \in U(\mathcal{Y})$ unitaire telle que $\forall i \in \{1, ..., d\} : U f_i = \bar{f}_i$

Propriété 13. *On a:*

$$\Psi = \sum_{1 \leq j \leq d} \bar{e}_j \otimes \bar{f}_j$$

où $\bar{e}_j$ est défini par: $\bar{e}_j = \sum_i \bar{f}_j^\star U \bar{f}_i e_i$ est une base orthonormée de $\mathcal{X}$

preuve. on a successivement:

$$\Psi = \sum_i e_i \otimes f_i = \sum_i e_i \otimes U^\star \bar{f}_i$$

$$= \sum_{ij} e_i \otimes \bar{f}_j \bar{f}_j^\star U^\star \bar{f}_i = \sum_j \left(\sum_i \bar{f}_j^\star U \bar{f}_i e_i \right) \otimes \bar{f}_j$$

□

Ainsi, si Alice effectue, sur son registre, la mesure associée à la base $\{\bar{e}_i\}$, alors, après cette mesure, l'état du registre de Bob est un des vecteur de la base $\{\bar{f}_i\}$

3.2 généralisation aux opérateurs densité

Alice prépare l'état $\rho^{AB} \in D(\mathcal{X} \otimes \mathcal{Y})$ et envoie le registre Y à Bob.
Alice veut agir à distance sur l'état de Bob en effectuant des mesures sur son registre (X) (POVM $\mu(a|x) \geq 0, \forall x \in \{1, ..., m\} : \sum_{1 \leq a \leq n} \mu(a|x) = \mathrm{Id}$)

Elle peut effectuer m mesures, et chaque mesure fournit un numéro entre 1 et n. voir [4] et [5]

La procédure est la suivante:

1) Alice prépare l'état $\rho^{AB} \in D(\mathcal{X} \otimes \mathcal{Y})$, et envoie le registre Y à Bob.

2) Bob demande à Alice d'effectuer la mesure $x \in \{1, ..., m\}$

3) Alice effectue cette mesure et retourne le résultat $a \in \{1, ..., n\}$ à Bob

4) Ils répètent ce schéma un nombre $N >> 1$ de fois, de façon indépendantes.

à la 1ère étape, Alice et Bob partagent ρ^{AB}, l'état effectif de Bob est $\rho^B = \mathrm{Tr}_1 \rho^{AB}$

Bob choisi x aléatoirement, suivant la distribution de probabilité $p(x)$

La probabilité d'obtenir a avec la mesure x est:

$$p(a|x) = \mathrm{Tr}_1 \left[\mu(a|x)\rho^A\right] = \mathrm{Tr}_{12} \left[(\mu(a|x) \otimes \mathrm{Id})\, \rho^{AB}\right]$$

si ayant mesuré x, Alice obtient a; l'état total devient:

$$\frac{\left(\mu(a|x)^{1/2} \otimes \mathrm{Id}\right) \rho^{AB} \left(\mu(a|x)^{1/2} \otimes \mathrm{Id}\right)}{\mathrm{Tr}\left[(\mu(a|x) \otimes \mathrm{Id})\, \rho^{AB}\right]}$$

Donc, l'état de Bob est:

$$\rho_{a|x} = \frac{\mathrm{Tr}_1 \left[(\mu(a|x) \otimes \mathrm{Id})\, \rho^{AB}\right]}{\mathrm{Tr}\left[(\mu(a|x) \otimes \mathrm{Id})\, \rho^{AB}\right]}$$

si Bob ne regarde pas le résultat d'Alice, alors, ce résultat étant aléatoire, l'état effectif de Bob est:

$$\sum_a \rho_{a|x} p(a|x) = \sum_a \mathrm{Tr}_1 \left[(\mu(a|x) \otimes \mathrm{Id})\, \rho_{AB}\right] = \mathrm{Tr}_1 \rho^{AB} = \rho^B$$

$\Rightarrow$ l'état de Bob est inchangé (pas de signal).

Cependant, si Bob tient compte des résultats de mesures d'Alice et qu'il partitionne ses registres en fonction de la valeur du couple (a, x), il obtient par tomographie connaissance des états $\rho_{a|x}$.

On défini: $\eta(a|x) = \mathrm{Tr}_1 \left[(\mu(a|x) \otimes \mathrm{Id})\, \rho^{AB}\right]$
d'où:

$$\rho_{a|x} = \frac{\eta(a|x)}{\mathrm{Tr}\, \eta(a|x)}$$

$$p(a|x) = \mathrm{Tr}\,\eta(a|x)$$
$$\forall x, \sum_a \eta(a|x) = \rho^B$$

Dans ce schéma, Alice influence l'état de Bob. Cependant, Bob est méfiant, il veut être certain que Alice a une influence non locale.
Dans ce but, il doit montrer que les états $\rho_{a|x}$ qu'il obtient ne sont pas explicables par un modèle à variables cachées locales. Voir [4]

3.3 Modèle à varable cachée locale :

Si Alice ne peut pas modifier l'état de Bob uniquement par des mesures sur son propre registre; elle peut toutefois:

1) tricher en ne préparant pas toujours le même état.
elle fournit à Bob l'état σ_λ avec λ connu de Alice. (σ_λ est préparé avec une probabilité $p(\lambda)$)

2) biaiser les statistique de Bob avec la réponse à la question x
Bob lui pose la question x, Alice connaissant λ et x répond a avec la probabilité $p(a|x,\lambda)$

Cherchons, dans ce modèle, quels sont les états $\rho_{a|x}$:
Bob ne connait pas λ et Alice choisit λ avant de connaître x, il choisit donc x indépendamment de λ:

$$p(\lambda, x) = p(\lambda)p(x)$$

L'état de Bob est (après avoir demandé x et reçu a).

$$\rho_{a|x} = \sum_\lambda p(\lambda|a,x)\sigma_\lambda$$
$$= \frac{\sum_\lambda p(\lambda)p(x)p(a|\lambda,x)\sigma_\lambda}{\sum_\mu p(\mu)p(x)p(a|\mu,x)} = \frac{\eta(a|x)}{\mathrm{Tr}\,\eta(a|x)} \text{ (Bayes)}$$
$$\text{avec: } \eta(a|x) = \sum p(\lambda)p(a|\lambda,x)\sigma_\lambda$$

on a:

$$p(a|x) = \mathrm{Tr}\,\eta(a|x)$$

Ainsi, si Bob après ses tomographies obtient les opérateurs $\eta(a|x) = p(a|x)\rho_{a|x}$ définis plus haut; et que il existe deux lois de probabilités $p(\lambda)$ et $p(a|\lambda,x)$ et des états σ_λ tels que:

$$\eta(a|x) = \sum_\lambda p(\lambda)p(a|\lambda,x)\sigma_\lambda$$

Alors Bob peut expliquer l'influence d'Alice avec un modèle à variables cachées locales, et il n'est pas convaincu par l'action à distance d'Alice.

A contrario, si un tel modèle est impossible, alors Bob est certain qu'Alice a au moins une influence non locale sur son registre.

3.4 lien entre le guidage et l'incompatibilité

montrons d'abord la proposition suivante:(cf [8] exercice 2.2)

Propriété 14. *soient X le registre d'Alice, Y le registre de Bob, $\rho_B \in D(\mathcal{Y})$, $u \in \mathcal{X} \otimes \mathcal{Y}$ tel que: $\mathrm{Tr}_{\mathcal{X}}(uu^\star) = \rho_B$ alors:*
pour toute famille $\{\eta(a)\}_{1\leq a\leq N} \in \mathrm{Pos}(\mathcal{Y})$ telle que:

$$\sum_{1\leq a\leq N} \eta(a) = \rho_B$$

il existe un POVM $\{\mu(a)\}_{0\leq a\leq N} \in \mathrm{Pos}(\mathcal{X})$ sur le registre X, tel que:

$$\forall a \in \{1,...,N\} : \mathrm{Tr}_{\mathcal{X}}\left[(\mu(a)\otimes \mathrm{Id}_{\mathcal{Y}})\, uu^\star\right] = \eta(a)$$

et

$$\mathrm{Tr}_{\mathcal{X}}\left[(\mu(0)\otimes \mathrm{Id}_{\mathcal{Y}})\, uu^\star\right] = 0$$

preuve. en effet:
on décompose u en Schmidt: $u = \sum_{1\leq i\leq r} \alpha_i v_i \otimes w_i$ avec $\forall i : \alpha_i > 0$, $\{v_i\}_{1\leq i\leq r}$ et $\{w_i\}_{1\leq i\leq r}$ étant des familles orthonormées.
soit V le sous espace engendré par $\{v_i\}_{1\leq i\leq r}$
on pose $\Pi_{V^\perp}$ = le projecteur orthogonal sur $V^\perp$
la condition $\sum_{1\leq a\leq N} \eta(a) = \rho_B$ implique que $\forall 1 \leq a \leq N : \mathrm{Im}\,\eta(a) \subset \mathrm{Im}\,\rho_B$
or

$$\rho_B = \mathrm{Tr}_{\mathcal{X}}(uu^\star) = \sum_{1\leq i\leq r} \alpha_i^2 w_i w_i^\star$$

$$\Rightarrow \eta(a) = \sum_{1\leq k,l\leq r} \eta_{kl}(a) w_k w_l^\star$$

Définissons

$$\begin{cases} \mu(0) = \Pi_{V^\perp} \\ \forall 1 \leq a \leq N : \mu(a) = \sum_{1\leq i,j\leq r} \alpha_i^{-1}\alpha_j^{-1}\eta_{ji}(a) v_i v_j^\star \end{cases}$$

$\{\mu(a)\}_{0\leq a\leq N}$ est le POVM cherché.
clairement $\mu(0) \geq 0$
aussi $\mu(a) \geq 0$ car puisque $\eta(a) \geq 0$, on a : $x^\star\mu(a)x = \sum_{1\leq i,j\leq r} \alpha_i^{-1}\alpha_j^{-1}\bar{x}_i x_j \eta_{ji} = \sum_{1\leq i,j\leq r} \alpha_j^{-1}\bar{\bar{x}}_j \eta_{ji}\alpha_i^{-1}\bar{x}_i \geq 0$

ensuite, la condition:

$$\sum_{1\leq a\leq N}\eta(a)=\rho_B$$

$$\iff \sum_{1\leq k,l\leq r} w_k w_l^\star \sum_{1\leq a\leq N}\eta_{kl}(a)=\sum_{1\leq i\leq r}\alpha_i^2 w_i w_i^\star$$

$$\iff \forall 1\leq k,l\leq r:\sum_{1\leq a\leq N}\eta_{kl}(a)=\delta_{kl}\alpha_k\alpha_l$$

donc:

$$\sum_{0\leq a\leq N}\mu(a)=\Pi_{V^\perp}+\sum_{1\leq a\leq N}\sum_{1\leq i,j\leq r}\alpha_i^{-1}\alpha_j^{-1}\eta_{ji}(a)v_i v_j^\star$$

$$=\Pi_{V^\perp}+\sum_{1\leq i,j\leq r}\alpha_i^{-1}\alpha_j^{-1}\delta_{ji}\alpha_i\alpha_j v_i v_j^\star$$

$$=\Pi_{V^\perp}+\sum_{1\leq i\leq r}v_i v_i^\star=\Pi_{V^\perp}+\Pi_V=\mathrm{Id}_{\mathcal{X}}$$

i.e. c'est bien un POVM.

enfin: $\forall a\in\{1,...,N\}$

$$\mathrm{Tr}_{\mathcal{X}}\left[(\mu(a)\otimes\mathrm{Id}_{\mathcal{Y}})\,uu^\star\right]=\mathrm{Tr}_{\mathcal{X}}\left[\left(\sum_{1\leq i,j\leq r}\alpha_i^{-1}\alpha_j^{-1}\eta_{ji}(a)v_i v_j^\star\otimes\mathrm{Id}_{\mathcal{Y}}\right)\sum_{1\leq k,l\leq r}\alpha_k\alpha_l v_k v_l^\star\otimes w_k w_l^\star\right]$$

$$=\sum_{1\leq i,j,k,l\leq r}\alpha_i^{-1}\alpha_j^{-1}\alpha_k\alpha_l\eta_{ji}(a)\delta_{jk}\delta_{il}w_k w_l^\star=\sum_{1\leq k,l\leq r}\eta_{kl}(a)w_k w_l^\star=\eta(a)$$

et aussi:

$$\mathrm{Tr}_{\mathcal{X}}\left[(\mu(0)\otimes\mathrm{Id}_{\mathcal{Y}})\,uu^\star\right]=0$$

□

soit maintenant $\{\eta(a|x)\}_{(x,a)\in\{1,...,m\}\times\{1,...,n\}}$ un assemblage de ρ_B, i.e.

$$\forall(x,a)\in\{1,...,m\}\times\{1,...,n\}:\eta(a|x)\geq 0$$

$$\forall 1\leq x\leq m:\sum_{1\leq a\leq n}\eta(a|x)=\rho_B$$

grâce à la proposition précedente, à cet assemblage est associé une famille de POVM

$$\{\mu(a|x)\}_{1\leq x\leq n\text{ et }0\leq a\leq n}$$

tq:

$$\mathrm{Tr}_{\mathcal{X}}\left[(\mu(a|x)\otimes\mathrm{Id}_{\mathcal{Y}})\,uu^\star\right]=\eta(a|x)(1-\delta_{0a})$$

Propriété 15. *Si $\eta(a|x)$ est un assemblage non guidable de ρ_B, alors, les POVM $\mu(.|x)$ sont compatibles.*

preuve. supposer que $\{\eta(a|x)\}_{x,a}$ est non guidable est équivalent à l'existence d'une décomposition de la forme $\forall(x,a) \in \{1,...m\} \times \{1,...,n\}$:

$$\eta(a|x) = \sum_{1\leq\lambda\leq L} p(\lambda)p(a|\lambda,x)\sigma_\lambda$$

comme expliqué plus haut.
d'où:

$$\mu(a|x) = \sum_{1\leq i,j\leq r} \alpha_i^{-1}\alpha_j^{-1}\eta_{ji}(a|x)v_i v_j^\star$$

$$= \sum_{1\leq\lambda\leq L} p(a|\lambda,x) \sum_{1\leq i,j\leq r} \alpha_i^{-1}\alpha_j^{-1}p(\lambda)(\sigma_\lambda)_{ji}v_i v_j^\star$$

$$\mu(0|x) = \Pi_{V^\perp}$$

donc, si l'on définis:

$$B_0 = \Pi_{V^\perp}$$

$$B_\lambda = \sum_{1\leq i,j\leq r} \alpha_i^{-1}\alpha_j^{-1}p(\lambda)(\sigma_\lambda)_{ji}v_i v_j^\star$$

$$q(a|x,\lambda) = \begin{cases} p(a|x,\lambda) \text{ si } 1\leq\lambda\leq L \text{ et } 1\leq a\leq n \\ 0 \text{ si } 1\leq\lambda\leq L \text{ et } a=0 \\ 0 \text{ si } \lambda=0 \text{ et } 1\leq a\leq n \\ 1 \text{ si } \lambda=0 \text{ et } a=0 \end{cases}$$

Alors, $\forall 0\leq a\leq x, 1\leq x\leq m$

$$\mu(a|x) = \sum_{0\leq\lambda\leq L} q(a|x,\lambda)B_\lambda$$

avec $\{B_\lambda\}_{0\leq\lambda\leq L}$ POVM, et $q(a|x,\lambda)$ est une loi de probabilité; parconséquent, les POVM $\{\eta(.|x)\}$ sont compatibles.

Pour montrer que $\{B_\lambda\}_{0\leq\lambda\leq L}$ est un POVM, on procède comme suit:

$$\mathrm{Id}_\mathcal{X} = \sum_{0\leq a\leq n} \mu(a|x) = \sum_{0\leq a\leq n}\sum_{0\leq\lambda\leq L} q(a|x,\lambda)B_\lambda = \sum_{0\leq\lambda\leq L}\sum_{0\leq a\leq n} q(a|x,\lambda)B_\lambda = \sum_{0\leq\lambda\leq L} B_\lambda$$

□

réciproquement, étant donné une famille de POVM $\mu(.|x)$, on définis un assemblage $\eta(.|x)$ de ρ_B par:

$$\eta(a|x) = \mathrm{Tr}_\mathcal{X}\left[(\mu(a|x)\otimes \mathrm{Id}_\mathcal{Y})\, uu^\star\right]$$

Propriété 16. *Si les $\mu(.|x)$ sont compatibles, alors $\eta(.|x)$ est non guidable*

preuve. effectivement, si $\forall 0 \leq a \leq n, 1 \leq x \leq m$

$$\mu(a|x) = \sum_{1 \leq \lambda \leq L} p(a|x,\lambda) B_\lambda$$

alors:

$$\eta(a|x) = \sum_{1 \leq \lambda \leq L} p(a|x,\lambda) \operatorname{Tr}\left[(B_\lambda \otimes \mathrm{Id}_\mathcal{Y})\, uu^\star\right] \frac{\operatorname{Tr}_\mathcal{X}\left[(B_\lambda \otimes \mathrm{Id}_\mathcal{Y})\, uu^\star\right]}{\operatorname{Tr}\left[(B_\lambda \otimes \mathrm{Id}_\mathcal{Y})\, uu^\star\right]}$$

ce qui montre que $\{\eta(.|x)\}$ est non guidable. □

4 Critère d'incompatibilité (Zhu)

Voir les articles [1] et [2]

Si $\vec{v}, \vec{p} \in \mathbb{R}^{+n}$ et f convexe $f : \mathbb{R} \to \mathbb{R}$
on définis:

$$D_f(\vec{v}||\vec{p}) = \sum_k p_k f(\frac{v_k}{p_k})$$

Propriété 17. *Pour toute matrice stochastique* Λ, $D_f(\Lambda\vec{v}||\Lambda\vec{p}) \leq D_f(\vec{v}||\vec{p})$

preuve. En effet:

$$\begin{aligned} D_f(\Lambda\vec{v}||\Lambda\vec{p}) &= \sum_i (\Lambda\vec{p})_i \, f\left(\frac{(\Lambda\vec{v})_i}{(\Lambda\vec{p})_i}\right) \\ &= \sum_i (\Lambda\vec{p})_i f\left(\sum_j \frac{\Lambda_{i,j} p_j}{(\Lambda\vec{p})_i} \frac{v_j}{p_j}\right) \\ &\leq \sum_i (\Lambda\vec{p})_i \sum_j \frac{\Lambda_{i,j} p_j}{(\Lambda\vec{p})_i} f\left(\frac{v_j}{p_j}\right) \\ &= \sum_j p_j f\left(\frac{v_j}{p_j}\right) = D_f(\vec{v}||\vec{p}) \end{aligned}$$

□

Si on prend $f(x) = x^2 : D_f = D_2$

$$D_2(\vec{v}||\vec{p}) = \sum_k p_k \left(\frac{v_k}{p_k}\right)^2 = \sum_k \frac{v_k^2}{p_k}$$

C'est l'entropie relative de Rényi.

Soit deux ensembles $\{\eta(a)\}, \{\theta(b)\}, \forall a, b : \eta(a), \theta(b) \geq 0$ représentant un même état ρ, i.e. $\sum_a \eta(a) = \sum_b \theta(b) = \rho$

On écrit $\vec{\eta} = \{\eta(a)\}$, et $\vec{\theta} = \{\theta(b)\}$; ainsi que $\vec{\eta} \prec \vec{\theta}$ lorsque il existe une application stochastique $p(a|b)$ telle que:

$$\forall a : \eta(a) = \sum_b p(a|b)\theta(b)$$

Soit deux assemblages $\{\eta(a|x)\}, \{\theta(b|y)\},$ que l'on abrègent en: $(\overleftrightarrow{\eta}, \overleftrightarrow{\theta})$
On écrit

$$\overleftrightarrow{\eta} \prec \overleftrightarrow{\theta} \text{ si } \forall x \exists y; \vec{\eta}(x) \prec \vec{\theta}(y)$$

Pour le guidage: soit $\overleftrightarrow{\eta}$ un assemblage de ρ_B, Alice guide Bob ssi pour tout ensemble $\vec{\theta}$ représentant ρ_B, on a: $\forall x : \vec{\eta}_x \not\prec \vec{\theta}$

$\forall Q \in \mathrm{Pd}(\mathcal{X})$, on définis:

$$G_Q(\vec{\eta}) = \sum_a \frac{|\eta(a)\rangle\rangle\langle\langle\eta(a)|}{\langle Q, \eta(a)\rangle}$$

Où étant fixé une base e_i de $\mathcal{X}$, on définit l'application $e_i e_j^\star \to |e_i e_j^\star\rangle\rangle = e_i \otimes e_j$; que l'on étend ensuite à $L(\mathcal{X})$ par linéarité ($\langle\langle e_i e_j^\star| = e_i^\star \otimes e_j^\star$) on renvoie à [8] pages 23-24 pour plus de détails.

Pour $Q > 0$ fixé, G_Q conserve l'ordre:

Propriété 18. *Pour toute paire d'ensemble $(\vec{\eta}, \vec{\theta})$ représentant un même état ρ :*

$$\vec{\eta} \prec \vec{\theta} \Rightarrow G_Q(\vec{\eta}) \leq G_Q(\vec{\theta})$$

preuve. En effet, si $\forall a; \eta(a) = \sum_b \Lambda_{ab}\theta(b)$ avec Λ stochastique, Alors $\forall C \in L(\mathcal{X})$:

$$\langle\langle C|G_Q(\vec{\eta})|C\rangle\rangle = \sum_a \frac{|\langle C, \eta(a)\rangle|^2}{\langle Q, \eta(a)\rangle}$$

$$= \sum_a \langle Q, \eta(a)\rangle \left| \sum_b \frac{\Lambda_{ab}\langle Q, \theta(b)\rangle}{\langle Q, \eta(a)\rangle} \frac{\langle C, \theta(b)\rangle}{\langle Q, \theta(b)\rangle} \right|^2$$

$$\leq \sum_a \langle Q, \eta(a)\rangle \left(\sum_b \frac{\Lambda_{ab}\langle Q, \theta(b)\rangle}{\langle Q, \eta(a)\rangle} \frac{|\langle C, \theta(b)\rangle|}{\langle Q, \theta(b)\rangle} \right)^2$$

$$\leq \sum_a \langle Q, \eta(a)\rangle \sum_b \frac{\Lambda_{ab}\langle Q, \theta(b)\rangle}{\langle Q, \eta(a)\rangle} \frac{|\langle C, \theta(b)\rangle|^2}{\langle Q, \theta(b)\rangle^2}$$

$$= \sum_b \frac{|\langle C, \theta(b)\rangle|^2}{\langle Q, \theta(b)\rangle} = \langle\langle C|G_Q(\vec{\theta})|C\rangle\rangle$$

$$\Rightarrow G_Q(\vec{\eta}) \leq G_Q(\vec{\theta})$$

□

On défini

$$R_Q : \mathcal{X} \otimes \mathcal{X} \to \mathcal{X} \otimes \mathcal{X}$$

par:

$$\forall S \in L(\mathcal{X}) : R_Q|S\rangle\rangle = \frac{1}{2}|SQ + QS\rangle\rangle$$

Propriété 19. $R_Q \geq 0$

preuve. $\forall S \in L(\mathcal{X})$

$$\langle\langle S|R_Q|S\rangle\rangle = \frac{1}{2}\langle\langle S|SQ + QS\rangle\rangle = \frac{1}{2}\operatorname{Tr} S^\star SQ + \operatorname{Tr} S^\star QS$$

$$= \frac{1}{2}\left(\underbrace{\operatorname{Tr} SQS^\star}_{\geq 0} + \underbrace{\operatorname{Tr} S^\star QS}_{\geq 0}\right) \geq 0$$

$\Rightarrow R_Q$ est positif.

□

Propriété 20.

$$\operatorname{Tr}\left[R_Q G_Q(\vec{\eta})\right] \leq \operatorname{Tr}\rho_B$$

avec égalité si et seulement si $\forall a; \operatorname{rank}\eta(a) = 1$

preuve.

$$\operatorname{Tr}\left[R_Q G_Q(\vec{\eta})\right] = \operatorname{Tr}\left[R_Q \sum_a \frac{|\eta(a)\rangle\rangle\langle\langle\eta(a)|}{\langle Q, \eta(a)\rangle}\right]$$

$$= \frac{1}{2}\sum_a \frac{1}{\langle Q, \eta(a)\rangle} \operatorname{Tr}\left[|\eta(a)Q + Q\eta(a)\rangle\rangle\langle\langle\eta(a)|\right]$$

$$= \sum_a \frac{\operatorname{Tr}\left[Q\eta(a)^2\right]}{\operatorname{Tr}\left[Q\eta(a)\right]}$$

Soit $X = \frac{\eta(a)}{\operatorname{Tr}\eta(a)}$, on a: $0 < X \leq \mathrm{Id} \Rightarrow X^2 \leq X$

$$\Rightarrow \frac{\operatorname{Tr} Q\eta(a)^2}{(\operatorname{Tr}\eta(a))^2} = \operatorname{Tr} QX^2 \leq \operatorname{Tr} QX = \frac{\operatorname{Tr} Q\eta(a)}{\operatorname{Tr}\eta(a)}$$

$$\Rightarrow \frac{\operatorname{Tr} Q\eta(a)^2}{\operatorname{Tr} Q\eta(a)} \leq \operatorname{Tr}\eta(a)$$

d'où:

$$\operatorname{Tr}\left[R_Q G_Q(\vec{\eta})\right] \leq \sum_a \operatorname{Tr}\eta(a) = \operatorname{Tr}\rho_B$$

si $\forall a : \operatorname{rank}\eta(a) = 1,$ alors, $\eta(a) = \lambda\sigma(a)$ avec $\lambda > 0$ et $\sigma(a) \in D(\mathcal{X}),$ tel que: $\sigma(a)^2 = \sigma(a)$

$$\Rightarrow \frac{\operatorname{Tr} Q\eta(a)^2}{\operatorname{Tr} Q\eta(a)} = \frac{\lambda^2}{\lambda}\frac{\operatorname{Tr} Q\sigma(a)^2}{\operatorname{Tr} Q\sigma(a)} = \lambda = \operatorname{Tr}\eta(a)$$

$$\Rightarrow \operatorname{Tr}\left[R_Q G_Q(\vec{\eta})\right] = \operatorname{Tr}\rho_B$$

réciproquement, si $\operatorname{Tr}\left[R_Q G_Q(\vec{\eta})\right] = \operatorname{Tr}\rho_B$, alors:

$$\forall a : \frac{\operatorname{Tr} Q\eta(a)^2}{\operatorname{Tr} Q\eta(a)} = \operatorname{Tr}\eta(a)$$

$$\Rightarrow \forall a : \frac{\operatorname{Tr} Q\eta(a)^2}{(\operatorname{Tr}\eta(a))^2} = \frac{\operatorname{Tr} Q\eta(a)}{\operatorname{Tr}\eta(a)}$$

$$\Rightarrow \forall a : \operatorname{Tr} QX_a^2 = \operatorname{Tr} QX_a$$

$$\Rightarrow \forall a : \operatorname{Tr} Q(X_a - X_a^2) = 0$$

$$\Rightarrow \forall a : \operatorname{Tr} Q^{1/2}(X_a - X_a^2)Q^{1/2} = 0$$

or $X_a - X_a^2 \geq 0 \Rightarrow Q^{1/2}(X_a - X_a^2)Q^{1/2} \geq 0$

$$\Rightarrow \forall a : Q^{1/2}(X_a - X_a^2)Q^{1/2} = 0$$

$$\Rightarrow \forall a : X_a - X_a^2 = 0$$

$$\Rightarrow \forall a : X_a^2 = X_a \Rightarrow \forall a : \operatorname{rank}\eta(a) = 1$$

□

Propriété 21. *On a:*

$$\operatorname{Tr}\left[G_{\mathrm{Id}}(\vec{\eta})\right] = \sum_a \frac{\operatorname{Tr}\eta(a)^2}{\operatorname{Tr}\eta(a)} \leq \operatorname{Tr}\rho_B$$

preuve. En effet: $R_{\mathrm{Id}_{\mathcal{X}}} = \mathrm{Id}_{L(\mathcal{X})}$ et égalité ssi $\forall a : \operatorname{rank}\eta(a) = 1$ □

Propriété 22. *On a (avec $Q = \mathrm{Id}$):*

$$G(\vec{\eta}) \geq \frac{|\rho_B\rangle\rangle\langle\langle\rho_B|}{\operatorname{Tr}\rho_B}$$

$$\operatorname{Tr} G(\vec{\eta}) \geq \frac{\operatorname{Tr}\rho_B^2}{\operatorname{Tr}\rho_B}$$

preuve. On utilise le fait que $\rho_B \prec \vec{\eta}$ □

Soit $\widetilde{G}_Q = R_Q^{1/2} G_Q R_Q^{1/2}$
on pose:

Définition 1.

$$\tau_Q(\overleftrightarrow{\eta}) = \inf\{\operatorname{Tr} F : F \geq \widetilde{G}_Q(\vec{\eta}(x))(\forall x)\}$$

Propriété 23.

$$\overleftrightarrow{\eta} \prec \overleftrightarrow{\theta} \Rightarrow \tau_Q(\overleftrightarrow{\eta}) \leq \tau_Q(\overleftrightarrow{\theta})$$

si $\overleftrightarrow{\eta}$ *est non guidable:*

$$\tau_Q(\overleftrightarrow{\eta}) \leq \operatorname{Tr} \rho_B$$

preuve.

$$\overleftrightarrow{\eta} \prec \overleftrightarrow{\theta} \iff \forall x \exists y : \vec{\eta}(x) \prec \vec{\theta}(y)$$

$$\text{si } \forall y : F \geq \widetilde{G}_Q(\vec{\theta}(y)) \text{ et } \tau_Q(\overleftrightarrow{\theta}) + \epsilon \geq \operatorname{Tr} F \geq \tau_Q(\overleftrightarrow{\theta})$$

alors $\forall x : F \geq \widetilde{G}_Q(\vec{\eta}(x)) \Rightarrow \operatorname{Tr} F \geq \tau_Q(\overleftrightarrow{\eta})$
donc $\tau_Q(\overleftrightarrow{\theta}) \geq \tau_Q(\overleftrightarrow{\eta})$

$\overleftrightarrow{\eta}$ non guidable $\iff \exists \vec{\theta}$ ensemble pour ρ_B tel que:

$$\forall x : \vec{\theta} \succ \vec{\eta}(x)$$

$$\Rightarrow \forall x, \forall Q \in \operatorname{Pd}(\mathcal{X}) : G_Q(\vec{\theta}) \geq G_Q(\vec{\eta}(x))$$

$\Rightarrow \forall x, \forall Q > 0 :$

$$R_Q^{1/2} G_Q(\vec{\theta}) R_Q^{1/2} \geq R_Q^{1/2} G_Q(\vec{\eta}_x) R_Q^{1/2}$$

d'un autre coté:

$$\operatorname{Tr}\left[R_Q^{1/2} G_Q(\vec{\theta}) R_Q^{1/2}\right] = \operatorname{Tr}\left[R_Q G_Q(\vec{\theta}_x)\right] \leq \operatorname{Tr} \rho_B$$

cela implique:

$$\tau_Q(\overleftrightarrow{\eta}) \leq \operatorname{Tr} \rho_B$$

□

on a le corollaire suivant:

Propriété 24. 1) *Si* $\overleftrightarrow{\eta} \prec \overleftrightarrow{\theta}$*, alors:*

$$\tau(\overleftrightarrow{\eta}) \leq \tau(\overleftrightarrow{\theta})$$

2) *Tout assemblage non guidable* $\overleftrightarrow{\eta}$ *satisfait à:*

$$\tau(\overleftrightarrow{\eta}) \leq \operatorname{Tr} \rho_B$$

Propriété 25. *Si* ρ_B *est inversible, alors:*
$\overleftrightarrow{\eta}$ *admet un raffinement d'ordre un ssi la famille de POVM* $\rho_B^{-1/2} \overleftrightarrow{\eta} \rho_B^{-1/2}$ *admet un 1-raffinement.*

Propriété 26. *Si* ρ_B *est inversible et si* $\overleftrightarrow{\eta}$ *assemblage de* ρ_B *admet un 1-raffinement, alors:*

$$\tau_Q(\rho_B^{-1/2} \overleftrightarrow{\eta} \rho_B^{-1/2}) \leq d$$

preuve. en effet, les POVM $\rho_B^{-1/2}\vec{\eta}_x\rho_B^{-1/2}$ sont 1-raffinables, on applique (23), en utilisant le fait que $\forall x : \sum_a \rho_B^{-1/2}\eta(a|x)\rho_B^{-1/2} = \mathrm{Id}$ et $\mathrm{Tr}\,\mathrm{Id} = d$ □

Propriété 27. *Tout ensemble $\vec{\eta}$ pour ρ_B satisfait à:*

$$G(\vec{\eta}) \leq R_{\rho_B}$$

preuve. $\forall C$ opérateur $C = A + iB$ avec A et B hermitiens.
on a que:

$$\langle\langle A+iB|G(\vec{\eta})|A+iB\rangle\rangle = \langle\langle A|G(\vec{\eta})|A\rangle\rangle + \langle\langle B|G(\vec{\eta})|B\rangle\rangle + i\left[\langle\langle A|G(\vec{\eta})|B\rangle\rangle - \langle\langle B|G(\vec{\eta})|A\rangle\rangle\right]$$

or avec A et B hermitiens

$$\langle\langle A|G(\vec{\eta})|B\rangle\rangle = \sum_a \frac{\langle A, \eta(a)\rangle\langle\eta(a), B\rangle}{\mathrm{Tr}\,\eta(a)} = \sum_a \frac{\langle B, \eta(a)\rangle\langle\eta(a), A\rangle}{\mathrm{Tr}\,\eta(a)} = \langle\langle B|G(\vec{\eta})|A\rangle\rangle$$

d'où:

$$\langle\langle C|G(\vec{\eta})|C\rangle\rangle = \langle\langle A|G(\vec{\eta})|A\rangle\rangle + \langle\langle B|G(\vec{\eta})|B\rangle\rangle$$

de la même manière,

$$\langle\langle C|R_{\rho_B}|C\rangle\rangle = \langle\langle A|R_{\rho_B}|A\rangle\rangle + \langle\langle B|R_{\rho_B}|B\rangle\rangle + i\left[\langle\langle A|R_{\rho_B}|B\rangle\rangle - \langle\langle B|R_{\rho_B}|A\rangle\rangle\right]$$

or:

$$\langle\langle A|R_{\rho_B}|B\rangle\rangle - \langle\langle B|R_{\rho_B}|A\rangle\rangle$$
$$= \frac{1}{2}\left(\mathrm{Tr}\left[A(\rho_B B + B\rho_B)\right] - \mathrm{Tr}\left[B(\rho_B A + A\rho_B)\right]\right) = 0$$
$$\Rightarrow \langle\langle C|R_{\rho_B}|C\rangle\rangle = \langle\langle A|R_{\rho_B}|A\rangle\rangle + \langle\langle B|R_{\rho_B}|B\rangle\rangle$$

finalement, pour tout A opérateur hermitiens:

$$\langle\langle A|G(\vec{\eta})|A\rangle\rangle = \sum_a \frac{\langle A, \eta(a)\rangle\langle\eta(a), A\rangle}{\mathrm{Tr}\,\eta(a)} = \sum_a \frac{\left|\langle A\eta(a)^{1/2}, \eta(a)^{1/2}\rangle\right|^2}{\langle\eta(a)^{1/2}, \eta(a)^{1/2}\rangle}$$

$$\leq \sum_a \langle A\eta(a)^{1/2}, A\eta(a)^{1/2}\rangle = \sum_a \mathrm{Tr}(A^2\eta(a)) = \mathrm{Tr}(A^2\rho_B)$$

$$= \frac{1}{2}\left(\mathrm{Tr}\,AA\rho_B + \mathrm{Tr}\,AA\rho_B\right) = \frac{1}{2}\left(\mathrm{Tr}\,AA\rho_B + \mathrm{Tr}\,A\rho_B A\right)$$

$$= \frac{1}{2}\left(\langle A, A\rho_B\rangle + \langle A, \rho_B A\rangle\right)$$

$$= \frac{1}{2}\langle\langle A|A\rho_B + \rho_B A\rangle\rangle = \langle\langle A|R_{\rho_B}|A\rangle\rangle$$

$$\forall A \text{ hermitien } \langle\langle A|G(\vec{\eta})|A\rangle\rangle \leq \langle\langle A|R_{\rho_B}|A\rangle\rangle$$

donc:
$\forall C$

$$\langle\langle C|G(\vec{\eta})|C\rangle\rangle = \langle\langle A|G(\vec{\eta})|A\rangle\rangle + \langle\langle B|G(\vec{\eta})|B\rangle\rangle \leq \langle\langle A|R_{\rho_B}|A\rangle\rangle + \langle\langle B|R_{\rho_B}|B\rangle\rangle = \langle\langle C|R_{\rho_B}|C\rangle\rangle$$
$$\Rightarrow G(\vec{\eta}) \leq R_{\rho_B}$$

□

Propriété 28. *Tout assemblage $\overleftrightarrow{\eta}$ pour ρ_B obéit à:*

$$\tau(\overleftrightarrow{\eta}) \leq d \operatorname{Tr} \rho_B$$

preuve. le numero (27) implique:

$$\tau(\overleftrightarrow{\eta}) \leq \operatorname{Tr} R_{\rho_B}$$

reste donc à calculer $\operatorname{Tr} R_{\rho_B}$
Pour tout $Q \geq 0, \operatorname{Tr} R_Q = d \operatorname{Tr} Q$
effectivement:

$$\operatorname{Tr} R_Q = \sum_{ij} \langle\langle E_{ij}|R_Q|E_{ij}\rangle\rangle = \frac{1}{2}\sum_{ij}\langle\langle E_{ij}|QE_{ij} + E_{ij}Q\rangle\rangle$$
$$= \frac{1}{2}\sum_{ij}\left(\operatorname{Tr}(E_{ji}QE_{ij}) + \operatorname{Tr}(E_{ji}E_{ij}Q)\right)$$
$$= \sum_{ij} \operatorname{Tr} E_{ii}Q = \sum_{ij} e_i^\star Q e_i = d \operatorname{Tr} Q$$

□

On s'intéresse au problème suivant:
étant donné $\{A_j\}_{1\leq j\leq n} \in \operatorname{Pos}(\mathcal{X})$
que vaux $t(\vec{A}) = \inf\{\operatorname{Tr} F | \forall j : F \geq A_j\}$?

Propriété 29. *Ce problème peut se formuler dans le cadre de la programmation semi-définie:*

$$\underline{Principal}$$
$$maximiser \sum_{1\leq i\leq n} \langle A_i, B_i\rangle$$
$$avec \{B_i\}_{1\leq i\leq n} \ tel \ que$$
$$\forall i : B_i \geq 0$$
$$\sum_i B_i = \operatorname{Id}_{\mathcal{X}}$$

$$\underline{Dual}$$
$$minimiser \ \operatorname{Tr} F$$
$$F \ tel \ que \ \forall i : F \geq A_i$$

preuve. (pour un résumé des définitions et résultats utilisés, cf [8] page 53)

en effet: soit $\{1, ..., n\} = S$

on pose:

$$\Phi : L(\mathbb{C}^S \otimes \mathcal{X}) \to L(\mathcal{X})$$

$$\Phi = \mathrm{Tr}_{\mathbb{C}^S}$$

$$A = \sum_i E_{ii} \otimes A_i \in \mathrm{Herm}(\mathbb{C}^S \otimes \mathcal{X})$$

$$B = \mathrm{Id}_{\mathcal{X}} \in \mathrm{Herm}(\mathcal{X})$$

l'action de Φ se calcule comme suit:

$$X \in L(\mathbb{C}^S \otimes \mathcal{X}) \Rightarrow \exists! \{B_{ij}\}_{i,j \in S} \in L(\mathcal{X}) \text{ tel que } X = \sum_{i,j \in S} e_i e_j^\star \otimes B_{ij}$$

$$\Rightarrow \Phi(X) = \sum_{i \in S} B_{ii}$$

$$X \geq 0 \Rightarrow B_{ii} \geq 0 (\forall i \in S)$$

$$\Phi(X) = \mathrm{Id}_{\mathcal{X}} \iff \sum_{i \in S} B_{ii} = \mathrm{Id}_{\mathcal{X}}$$

$$\langle A, X \rangle = \langle \sum_{i \in S} E_{ii} \otimes A_i, \sum_{j,k \in S} E_{jk} \otimes B_{jk} \rangle$$

$$= \mathrm{Tr}_{\mathbb{C}^S \otimes \mathcal{X}} \left[\sum_{i,k \in S} E_{ik} \otimes A_i B_{ik} \right] = \sum_{i \in S} \mathrm{Tr}\left[A_i B_{ii}\right] = \sum_{i \in S} \langle A_i, B_{ii} \rangle$$

d'où, $\forall X \in \mathcal{A} = \left\{ X \in \mathrm{Pos}\left(\mathbb{C}^S \otimes \mathcal{X}\right) : \Phi(X) = \mathrm{Id}_{\mathcal{X}} \right\}$
il existe un POVM $\{B_i\}_{i \in S}$ tel que si on défini $X = \sum_{i \in S} E_{ii} \otimes B_i$, alors:

$$\langle A, X \rangle = \sum_{i \in S} \langle A_i, B_i \rangle$$

Ainsi,

$$\sup_X \{\langle A, X \rangle | X \geq 0 \text{ et } \Phi(X) = \mathrm{Id}_{\mathcal{X}}\} = \sup_{\{B_i\}_{i \in S}} \left\{ \sum_{i \in S} \langle A_i, B_i \rangle | \{B_i\} \text{ POVM } \right\}$$

il faut aussi vérifier:

$$\inf_Y \{\langle \mathrm{Id}_{\mathcal{X}}, Y \rangle | \Phi^\star(Y) \geq A \text{ et } Y \in \mathrm{Herm}(\mathcal{X})\} = \inf_Y \{\mathrm{Tr}\, Y | \forall i \in S : Y \geq A_i\}$$

commençons par déterminer $\Phi^\star(Y)$

$$L(\mathbb{C}^S \otimes \mathcal{X}) \underset{\Phi^\star}{\overset{\Phi}{\rightleftarrows}} L(\mathcal{X})$$

$$\langle \Phi(X), Y \rangle = \langle X, \Phi^\star(Y) \rangle$$

Lemme. $\forall Y \in L(\mathcal{X}) : \Phi^\star(Y) = \sum_{i\in S} E_{ii} \otimes Y$

preuve. $\forall X \in L(\mathbb{C}^S \otimes \mathcal{X})$:

$$\langle \Phi(X), Y\rangle = \mathrm{Tr}_{\mathcal{X}} \left[\sum_i B_{ii}^\star Y\right]$$

et, $\langle X, \Phi^\star(Y)\rangle =$

$$\mathrm{Tr}_{\mathbb{C}^S\otimes\mathcal{X}} \left[\left(\sum_{ij} E_{ij}\otimes B_{ij}\right)^\star \left(\sum_k E_{kk}\otimes Y\right)\right] = \mathrm{Tr}_{\mathbb{C}^S\otimes\mathcal{X}} \left[\sum_{ij} E_{ji}\otimes B_{ij}^\star Y\right] = \mathrm{Tr}_{\mathcal{X}} \left[\sum_i B_{ii}^\star Y\right]$$

□

Enfin, $\Phi^\star(Y) \geq A \iff \sum_{i\in S} E_{ii}\otimes(Y - A_i) \geq 0$

$$\iff \forall i \in S : Y - A_i \geq 0$$

$\Rightarrow$ on a bien notre programme semi défini. □

On pose:

$$\mathcal{A} = \left\{X \in \mathrm{Pos}(\mathbb{C}^S \otimes X) \text{ tel que: } \Phi(X) = \mathrm{Id}_{\mathcal{X}}\right\}$$

$$\mathcal{B} = \{Y \in \mathrm{Herm}(X) \text{ tel que: } \Phi^\star(Y) \geq A\}$$

$$\alpha = \sup\{\langle A, X\rangle : X \in \mathcal{A}\}$$

$$\beta = \inf\{\langle B, Y\rangle : Y \in \mathcal{B}\}$$

Propriété 30.

$$-\infty < \alpha = \beta < +\infty$$

$$\exists X \in \mathcal{A} : \langle A, X\rangle = \alpha$$

$$\exists Y \in \mathcal{B} : \langle B, Y\rangle = \beta$$

preuve. l'existence de POVM $\{B_i\}_{1\leq i\leq n}$ implique que $\alpha > -\infty$
de plus, pour tout POVM $\{B_i\}_{1\leq i\leq n}$:

$$\sum_{i\in S}\langle A_i, B_i\rangle \leq \sum_{i\in S}\langle A_i, \mathrm{Id}_{\mathcal{X}}\rangle = \sum_{i\in S}\mathrm{Tr}\, A_i$$

$$\Rightarrow \alpha \leq \sum_{i\in S}\mathrm{Tr}\, A_i < +\infty$$

ensuite, on remarque que l'ensemble des F tels que $F \geq A_i$ pour tout i, est non vide.

$$\Rightarrow \beta < +\infty$$

de plus un tel F satisfait à: $\forall i \in S : \operatorname{Tr} F \geq \operatorname{Tr} A_i$

$$\Rightarrow \beta \geq \max_{i \in S} \operatorname{Tr} A_i > -\infty$$

maintenant, si on prend $Y = \operatorname{Id}_{\mathcal{X}} + \sum_{i \in S} A_i$, alors $\forall i \in S : Y > A_i \Rightarrow \sum_{i \in S} E_{ii} \otimes (Y - A_i) > 0 \Rightarrow \Phi^\star(Y) > A$
et si on choisi $X = \sum_{i \in S} E_{ii} \otimes \frac{\operatorname{Id}_{\mathcal{X}}}{|S|}$, alors $X > 0$, et $\Phi(X) = \operatorname{Id}_{\mathcal{X}}$

$\Rightarrow$ on est dans les conditions d'application du théorème de Slater ([8] théorème 1.18) □

soit $\{A_i\}_{i \in S} \in \operatorname{Pos}(\mathcal{X})$
et $t(\vec{A}) = \min \{\operatorname{Tr} F | F \geq A_i (\forall i)\}$

Propriété 31. $t(\vec{A}) \leq \sum_i \operatorname{Tr} A_i$

Propriété 32. $t(\vec{A}) = \sum_i \operatorname{Tr} A_i \iff$ *les A_i ont des support 2 à 2 orthogonaux.*

preuve. comme $t(\vec{A}) = \max \left\{ \sum_{i \in S} \langle A_i, B_i \rangle | \{B_i\} \text{ POVM } \right\}$, si les A_i ont des supports 2 à 2 orthogonaux, on prend $B_i =$ la projection orthogonale sur le support de A_i, on a:

$$B_i \geq 0, \ \sum_i B_i = \operatorname{Id} \text{ et } \sum_{i \in S} \operatorname{Tr} A_i B_i = \sum \operatorname{Tr} A_i$$

$$\Rightarrow t(\vec{A}) = \sum_i \operatorname{Tr} A_i$$

réciproquement, si $t(\vec{A}) = \sum_i \operatorname{Tr} A_i$
alors il existe un POVM $\{B_i\}_{i \in S}$ tel que:

$$\sum_{i \in S} \langle A_i, B_i \rangle = \sum_{i \in S} \langle A_i, \operatorname{Id} \mathcal{X} \rangle$$

$$\iff \sum_{i \in S} \langle A_i, B_i - \operatorname{Id}_{\mathcal{X}} \rangle = 0$$

$$\Rightarrow \forall i \in S : \langle A_i, \operatorname{Id}_{\mathcal{X}} - B_i \rangle = 0$$

$$\Rightarrow \forall i \in S : \operatorname{Im} A_i \perp \operatorname{Im}(\operatorname{Id}_{\mathcal{X}} - B_i)$$

$$\iff \operatorname{Im} A_i \subset \ker(\operatorname{Id}_{\mathcal{X}} - B_i)$$

or, $i \neq j \Rightarrow \ker(\operatorname{Id}_{\mathcal{X}} - B_i) \perp \ker(\operatorname{Id}_{\mathcal{X}} - B_j)$
en effet: si $x \in \ker(\operatorname{Id}_{\mathcal{X}} - B_i)$ et $y \in \ker(\operatorname{Id}_{\mathcal{X}} - B_j)$
alors $B_i x = x$ et $B_j y = y$
puisque $B_i + B_j \leq \operatorname{Id}_{\mathcal{X}}$, on a:

$$x^\star B_i x + x^\star B_j x \leq x^\star x$$

$$\iff x^\star x + x^\star B_j x \leq x^\star x$$
$$\iff x^\star B_j x \leq 0$$
$$\iff x^\star B_j x = 0$$
$$\iff B_j x = 0$$

donc, x est un vecteur propre de B_j de valeur propre $0 \neq 1$

$$\Rightarrow x \perp y$$

parconséquent: $i \neq j \Rightarrow \operatorname{Im} A_i \perp \operatorname{Im} A_j$ □

Propriété 33. *si les A_i sont 2 à 2 orthogonaux, alors:*

$$F \geq A_i (\forall i \in S) \text{ et } \operatorname{Tr} F = t(\vec{A}) \Rightarrow F = \sum_{i \in S} A_i$$

preuve. en effet: si $i \neq j \Rightarrow \operatorname{Im} A_i \perp \operatorname{Im} A_j$ alors $B_i = A_i^+ A_i = \Pi_i$ est un POVM tel que:

$$\sum_{i \in S} \langle A_i, B_i \rangle = \sum_{i \in S} \operatorname{Tr} A_i$$

i.e.

$$X = \sum_{i \in S} E_{ii} \otimes \Pi_i \in \mathcal{A} \text{ et } \langle A, X \rangle = \sum_{i \in S} \operatorname{Tr} A_i$$

si $F \geq A_i (\forall i \in S)$ et $\operatorname{Tr} F = t(\vec{A}) = \sum_{i \in S} \operatorname{Tr} A_i$, alors

$$F \in \mathcal{B}, \text{ et } \langle \mathrm{Id}_{\mathcal{X}}, F \rangle = \langle A, X \rangle$$
$$\Rightarrow \Phi^\star(F) X = AX \text{ (slackness) voir [8] théorème 1.19}$$
$$\iff \left(\sum_{i \in S} E_{ii} \otimes F \right) \left(\sum_{j \ inS} E_{jj} \otimes \Pi_j \right) = \left(\sum_{i \in S} E_{ii} \otimes A_i \right) \left(\sum_{j \ inS} E_{jj} \otimes \Pi_j \right)$$
$$\iff \sum_{i \in S} E_{ii} \otimes F\Pi_i = \sum_{i \in S} E_{ii} \otimes A_i \Pi_i = \sum_{i \in S} E_{ii} \otimes A_i$$
$$\iff \forall i \in S : F\Pi_i = A_i$$
$$\Rightarrow F = \sum_{i \in S} F\Pi_i = \sum_{i \in S} A_i$$

□

Propriété 34. *tout assemblage $\{\eta(a|x)\} = \overleftrightarrow{\eta}$ satisfait:*

$$\tau(\overleftrightarrow{\eta}) \leq \sum_x \operatorname{Tr} \left[G(\vec{\eta}(x)) \right] = \sum_{a,x} \frac{\operatorname{Tr} \eta(a|x)^2}{\operatorname{Tr} \eta(a|x)}$$

égalité ssi $(x \neq y \Rightarrow \forall a, b : \eta(a|x) \perp \eta(b|y))$

preuve.

$$\tau(\overleftrightarrow{\eta}) = \inf\{\operatorname{Tr} F : F \geq G(\vec{\eta}(x))(\forall x)\}$$
$$\Rightarrow \tau(\overleftrightarrow{\eta}) \leq \sum_x \operatorname{Tr}\left(G(\vec{\eta}(x))\right)$$

avec égalité ssi $x \neq y \Rightarrow G(\vec{\eta}(x)) \perp G(\vec{\eta}(y))$

$$\iff \left[x \neq y \Rightarrow \sum_a \frac{|\eta(a|x)\rangle\rangle\langle\langle\eta(a|x)|}{\operatorname{Tr}\eta(a|x)} \perp \sum_b \frac{|\eta(b|y)\rangle\rangle\langle\langle\eta(b|y)|}{\operatorname{Tr}\eta(b|y)}\right]$$

$$\iff [x \neq y \Rightarrow \forall a, b : \langle\langle\eta(a|x)||\eta(b|y)\rangle\rangle = 0]$$
$$\iff [x \neq y \Rightarrow \forall a, b : \eta(a|x) \perp \eta(b|y)]$$

□

Propriété 35. *Tout assemblage $\overleftrightarrow{\eta}$ pour ρ_B satisfait:*

$\tau(\overleftrightarrow{\eta}) \leq m \operatorname{Tr}\rho_B$ *égalité ssi:* $\left[\left[\forall a, b, x, y : x \neq y \Rightarrow \rho_{a|x} \perp \rho_{b|y}\right]\right.$ *et* $\left.\forall a, x : \operatorname{rank}\rho_{a|x} = 1\right]$
avec m le nombre de POVM qui constituent L'assemblage $\overleftrightarrow{\eta}$

preuve. on sait que:

$$\tau(\overleftrightarrow{\eta}) \leq \sum_x \operatorname{Tr}\left(G(\vec{\eta}(x))\right) \leq m \operatorname{Tr}\rho_B$$

la première inégalité est une égalité si et seulement si $x \neq y, \forall a, b : \eta(a|x) \perp \eta(b|y)$
la seconde est une égalité ssi $\forall a, x \operatorname{rank}\eta(a|x) = 1$ □

♣♢♡♠

References

[1] H. Zhu M. Hayashi L. Chen. Universal steering criterial. *Physical review letters*, 2016.

[2] H. Zhu M.Hayashi L. Chen. Universal steering inequalities: supplementary material. •, 2016.

[3] M. Nielsen I. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[4] H. Wiseman S. Jones A. Doherty. Steering, entanglement, nonlocality, and the epr paradox. *Physical review letters*, 2017.

[5] R. Uola A. Costa H. Chau-Nguyen O. Gühne. Quantum steering. 2019.

[6] F. Laloë. *Comprenons nous vraiment la mécanique quantique?* EDP sciences, 2011.

[7] H. Barnum C. Caves C. Fuchs R. Jozsa B. Schumacher. Noncommuting mixed states cannot be broadcast. *Physical review letters*, 1996.

[8] J. Watrous. *The theory of quantum information.* Cambridge university press, 2018.

[9] M. Wilde. *Quantum information theory.* Cambridge university press, 2013.

[10] T. Heinosaari T. Miyadera M. Ziman. An invitation to quantum incompatibility. *Journal of Physics*, 2016.