Introduction à la théorie de l'information quantique

Ion NECHITA

Juillet-Août 2005

---

sujet proposé par Stephane Attal

Table des matières

1 Introduction

Ce stage à été l'occasion de découvrir la théorie de l'information quantique, une théorie assez jeune qui date des années '80. Évidement, il a été nécessaire d'assimiler les bases de l'information classique et de la mécanique quantique : ces rappels sont regroupés dans deux appendices. Ensuite, on entre dans le coeur de la théorie : l'entropie de von Neumann et ses propriétés. On pense toujours aux équivalents classiques pour souligner l'étrangeté du quantique. On présente d'ailleurs un contre exemple pour un énoncé analogue au théorème de Kolmogorov. On parle aussi de l'effet des mesures de von Neumann sur l'entropie avec le cas de la dimension 2 détaillé.

L'avant dernière partie parle de la sous-additivité forte, une inégalité qui a fait l'histoire de la théorie. La preuve et une inégalité équivalente sont données. Pour finir, trois applications des plus étranges et en même temps des plus puissantes sont présentées.

2 Théorie de l'information quantique

2.1 L'entropie de von Neumann : définition, propriétés de base

Définition 2.1 (entropie de von Neumann). Soit ρ l'état d'un système quantique A. On définit l'entropie de A par l'égalité

$$S(A) = S(\rho) = -\operatorname{tr}(\rho \log \rho) \tag{2.1.1}$$

D'après la définition, on peut déduire l'expression de l'entropie dans une base où ρ est diagonale, c'est à dire on peut exprimer $S(\rho)$ en fonction des valeurs propres de ρ. Ce résultat est très important car il permet souvent de faciliter les calculs :

Proposition 2.2 (l'entropie comme fonction des valeurs propres). *Si les valeurs propres de ρ sont $\lambda_1, \ldots, \lambda_d$, alors l'entropie de von Neumann vaut*

$$S(\rho) = -\sum_{i=1}^{d} \lambda_i \log \lambda_i. \tag{2.1.2}$$

En particulier, l'entropie ne dépend que des valeurs propres de la matrice densité ρ.

Remarque 2.3. D'après cette proposition, l'entropie d'un état quantique ρ de valeurs propres λ_i est la même que celle de la distribution de probabilités $(\lambda_i)_i$. Donc, en principe, toute propriété démontrée pour l'entropie de von Neumann reste valable dans le cas classique, tout simplement en considérant des états diagonalisables dans une même base $(|e_i\rangle)_i$.

Quelques propriétés de base découlent immédiatement de la définition et des propriétés de l'entropie de Shannon :

Proposition 2.4 (positivité). *L'entropie $S(\rho)$ est toujours positive et vaut zéro si et seulement si l'état ρ est un état pur.*

Proposition 2.5 (sous-systèmes d'un état pur). *Soit AB un système composé, dans un état pur $|AB\rangle$. Alors, si on pose $S(\rho_A) = \operatorname{tr}_B(|AB\rangle\langle AB|)$ et $S(\rho_B) = \operatorname{tr}_A(|AB\rangle\langle AB|)$, on a $S(\rho_A) = S(\rho_B)$.*

Remarque 2.6. Même si l'état AB se trouve dans un état pur, il est possible que les parties A et B soient des états non-purs, ce qui n'a pas d'équivalent classique. Voir aussi la remarque 2.9

Proposition 2.7 (l'entropie d'un produit tensoriel).

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma).$$

On introduit maintenant, comme pour l'information classique, les notions d'entropie conditionnelle et d'entropie relative :

Définition 2.8 (entropie conditionnelle).

$$S(A|B) = S(A,B) - S(B). \tag{2.1.3}$$

Remarque 2.9. On trouve dans cette définition la première différence importante entre l'entropie de von Neumann et celle de Shannon, car l'entropie conditionnelle quantique n'est pas forcement positive. Pour s'en convaincre, considérons l'état $\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$. Comme il s'agit d'un état pur, d'après la proposition 2.4, on a $S(A,B) = 0$. Mais on sait très bien que $\rho_A = \rho_B = I/2$, et donc $S(A) = S(B) = \log 2 = 1$. On est donc ici en présence d'un cas extrême : $S(A|B) = S(B|A) = -\log 2 = -1$. Le fait d'avoir des entropies conditionnelles négatives n'a pas d'équivalent classique et constitue une des "curiosités" de la théorie de l'information quantique.

Proposition 2.10. *Un état pur $|AB\rangle$ est intriqué si et seulement si $S(A|B) < 0$.*

Définition 2.11 (entropie relative).

$$S(\rho\|\sigma) = \mathrm{tr}(\rho\log\rho) - \mathrm{tr}(\rho\log\sigma).$$

Remarque 2.12. Comme elle est définie, l'entropie relative quantique peut être infinie. Ceci arrive quand le support de ρ intersecte le noyau de σ.

Comme pour l'information classique, on a le résultat suivant :

Théorème 2.13 (Inégalité de Klein). *L'entropie relative est positive,*

$$S(\rho\|\sigma) \geq 0, \tag{2.1.4}$$

avec égalité si et seulement si $\rho = \sigma$.

Preuve. Il suffit d'exprimer ρ et σ dans leurs bases de vecteurs propres et procéder par calcul direct. □

Corollaire 2.14 (valeur maximale de l'entropie). Si la dimension de l'espace de Hilbert dans lequel un état quantique ρ vit est d, alors l'entropie $S(\rho)$ vaut au plus $\log d$, avec égalité si et seulement si $\rho = I/d$.

Preuve. Il suffit juste d'écrire $S(\rho||\ \frac{I}{d}) \geq 0$ et de remarquer que $-\mathrm{tr}(\rho\log\frac{I}{d}) = \log d$. □

Un autre résultat intéressant portant sur l'entropie relative est le suivant :

Proposition 2.15. *Soit ρ_{AB} l'état d'un système composé AB. Alors*

$$S(\rho_{AB}||\ \rho_A\otimes\rho_B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}).$$

Preuve. D'après la définition de l'entropie relative, il suffit de montrer que

$$\mathrm{tr}(\rho_{AB}\log(\ \rho_A\otimes\rho_B)) = \mathrm{tr}(\rho_A\log\rho_A) + \mathrm{tr}(\rho_B\log\rho_B).$$

En effet, comme $\log(\rho_A\otimes\rho_B) = \log(\rho_A)\otimes I_B + I_A\otimes\log(\rho_B)$, il nous reste juste à montrer que

$$S(\rho_A) = \mathrm{tr}(\rho_{AB}\log(\rho_A\otimes I_B)),$$

qui se démontre par calcul direct dans une base. □

Comme sa contrepartie classique, l'entropie de von Neumann est sous-additive :

Proposition 2.16 (sous-additivité).

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B), \tag{2.1.5}$$

avec égalité si et seulement si $\rho_{AB} = \rho_A \otimes \rho_B$.

Preuve. Par la proposition 2.15, $S(\rho_{AB}|| \ \rho_A \otimes \rho_B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$. Mais $S(\rho_{AB}|| \ \rho_A \otimes \rho_B) \geq 0$, avec égalité si et seulement si $\rho_{AB} = \rho_A \otimes \rho_B$, d'où la conclusion.

Proposition 2.17 (inégalité du triangle (ou de Araki-Lieb)).

$$S(\rho_{AB}) \geq |S(\rho_A) - S(\rho_B)|. \tag{2.1.6}$$

Preuve. Soit ABR une purification du système AB. En appliquant la sous-additivité au système AR, nous avons

$$S(\rho_{AR}) \leq S(\rho_A) + S(\rho_R),$$

ou encore

$$S(\rho_B) - S(\rho_A) \leq S(\rho_{AB}).$$

L'autre inégalité se démontre de la même façon. □

2.2 Application de l'entropie de Von Neumann

Dans cette partie on va utiliser l'entropie quantique pour répondre à la question suivante : Étant donnés deux états quantiques ρ_{AC} sur $\mathcal{H}_A \otimes \mathcal{H}_C$ et ρ_{BC} sur $\mathcal{H}_B \otimes \mathcal{H}_C$ tels que $\mathrm{tr}_A(\rho_{AC}) = \mathrm{tr}_B(\rho_{BC})$ (c'est à dire que la partie "C" est la même), existe-t-il un état ρ_{ABC} sur $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ tel qu'on ait $\rho_{AC} = \mathrm{tr}_B(\rho_{ABC})$ et $\rho_{BC} = \mathrm{tr}_A(\rho_{ABC})$?

Comme on va le voir, la réponse dans le cas général est non. On va démontrer d'abord quelques lemmes utiles :

Lemme 2.18. Soit ρ_{AB} un état quantique tel que $\rho_A = \mathrm{tr}_B(\rho_{AB})$ soit dans un état pur qu'on note $|a\rangle\langle a|$. Alors $\rho_{AB} = |a\rangle\langle a| \otimes \rho_B$, i.e. les parties A et B ne sont pas intriquées.

Preuve. En écrivant la sous-additivité et l'inégalité du triangle pour le système AB, on obtient respectivement :

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B) \tag{2.2.7}$$

et

$$S(\rho_{AB}) \geq S(\rho_B) - S(\rho_A). \tag{2.2.8}$$

Mais comme la partie A se trouve dans un état pur, on a $S(\rho_A) = 0$. On a donc égalité dans les deux inégalités précédentes, ce qui nous permet de conclure. □

Lemme 2.19. Soit ρ_{ABC} un état quantique tel que $\rho_{AC} = \mathrm{tr}_B(\rho_{ABC})$ et $\rho_{BC} = \mathrm{tr}_A(\rho_{ABC})$ se trouvent dans des états purs. Alors $\rho_{ABC} = |a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |c\rangle\langle c|$, i.e. les parties A, B et C ne sont pas intriquées et se trouvent dans des états purs.

Preuve. En effet, comme les parties AC et BC sont pures on peut utiliser le lemme précèdent. On a

$$\rho_{ABC} = |AC\rangle\langle AC| \otimes \rho_B \tag{2.2.9}$$

et

$$\rho_{ABC} = |BC\rangle\langle BC| \otimes \rho_A. \tag{2.2.10}$$

La première égalité nous permet d'écrire

$$\rho_{BC} = \rho_B \otimes \rho_C, \tag{2.2.11}$$

et donc

$$\rho_{ABC} = \rho_A \otimes \rho_B \otimes \rho_C. \tag{2.2.12}$$

Mais AC se trouve dans un état pur, donc

$$0 = S(\rho_{AC}) = S(\rho_A \otimes \rho_C) = S(\rho_A) + S(\rho_C).$$

C'est à dire que ρ_A et ρ_C sont des états d'entropie nulle, i.e. des états purs. De même, B se trouve dans un état pur. □

Ce deuxième résultat nous fournit le contre exemple pour la question de départ. En effet, il suffit de considérer des états AC et BC purs tels que C soit non-pur (par exemple des états de Bell). Le lemme précédent interdit l'existence d'un état ρ_{ABC} qui vérifie les hypothèses de notre question. Donc la réponse au problème de départ est bien non, comme annoncé.

2.3 Mesures et entropie

Ici on étudie l'effet des mesures quantiques sur l'entropie des états. Dans le cas de mesures de projection de von Neumann on a un résultat simple : l'entropie croît avec la mesure.

Proposition 2.20. *Soit ρ un opérateur densité et $(P_i)_i$ des opérateurs de projection. Si on ignore le résultat de la mesure, le nouveau état du système est $\rho' = \sum_i P_i \rho P_i$. Alors*

$$S(\rho') \geq S(\rho),$$

avec égalité si et seulement si $\rho' = \rho$.

Preuve. Par l'inégalité de Klein, $S(\rho||\rho') \geq 0$, qu'on peut réécrire $S(\rho) \leq -\operatorname{tr}(\rho \log \rho')$. Il suffit donc de montrer l'égalité $S(\rho') = -\operatorname{tr}(\rho \log \rho')$. En effet,

$$\begin{aligned}
\operatorname{tr}(\rho \log \rho') &= \operatorname{tr}(\sum_i P_i \rho \log \rho') \\
&= \operatorname{tr}(\sum_i P_i^2 \rho \log \rho') \\
&= \operatorname{tr}(\sum_i P_i \rho \log \rho' P_i) \\
&= \operatorname{tr}(\sum_i P_i \rho P_i \log \rho') \\
&= \operatorname{tr}(\rho' \log \rho').
\end{aligned}$$

Au passage on a utilisé le fait que $\log \rho'$ commute avec les P_i. Montrons-le :

$$P_i \rho' = P_i \sum_j P_j \rho P_j = P_i \rho P_i = \rho' P_i,$$

et donc, comme ρ' commute avec les P_i, $\log \rho'$ aussi. □

Dans le cas d'un système d'un seul qubit, la proposition précédente prend une forme plus simple, et sa réciproque est aussi vraie sous une hypothèse supplémentaire. On se place donc sur $\mathcal{H} = \mathbb{C}^2$ et on va utiliser systématiquement la représentation des opérateurs densités comme des vecteurs de Bloch :

$$\rho = \frac{I + \overrightarrow{r} \cdot \overrightarrow{\sigma}}{2}.$$

Dans la suite on va noter $r = \|\overrightarrow{r}\| = \sqrt{r_1^2 + r_2^2 + r_3^2}$.

Au passage on peut remarquer que l'entropie de von Neumann de l'état s'écrit comme une fonction de r. Pour calculer cette entropie $S(\rho)$, il faut trouver les valeurs propres de ρ. Un calcul simple nous donne

$$\lambda_1 = \frac{1-r}{2}, \quad \lambda_2 = \frac{1+r}{2}, \tag{2.3.13}$$

et donc

$$S(\rho) = -(\lambda_1 \log \lambda_1 + \lambda_2 \log \lambda_2) = S(r). \tag{2.3.14}$$

Il se trouve que $r \mapsto S(r)$ est une fonction croissante.

Comme on travaille dans $\mathbb{C}^2$, le seul choix possible pour les opérateurs de projection est de prendre les projections sur deux vecteurs orthogonaux de $\mathbb{C}^2$:

$$\begin{aligned} P_1 &= |u\rangle\langle u| = \frac{I + \overrightarrow{p} \cdot \overrightarrow{\sigma}}{2}, \\ P_2 &= I - P_1 = |u^\perp\rangle\langle u^\perp| = \frac{I - \overrightarrow{p} \cdot \overrightarrow{\sigma}}{2}. \end{aligned}$$

Comme P_1 est l'opérateur densité d'un état pur, on a bien évidement $p = \|\overrightarrow{p}\| = 1$. L'état du système après la mesure (dont on ignore le résultat) est représenté par l'opérateur densité

$$\rho' = P_1 \rho P_1 + P_2 \rho P_2,$$

qui s'écrit dans la base de Bloch comme

$$\rho' = \frac{I + \overrightarrow{s} \cdot \overrightarrow{\sigma}}{2},$$

avec

$$\begin{aligned} s_1 &= p_1(p_1 r_1 + p_2 r_2 + p_3 r_3), \\ s_2 &= p_2(p_1 r_1 + p_2 r_2 + p_3 r_3), \\ s_3 &= p_3(p_1 r_1 + p_2 r_2 + p_3 r_3). \end{aligned} \tag{2.3.15}$$

Si on note $\overrightarrow{p} \cdot \overrightarrow{r} = p_1 r_1 + p_2 r_2 + p_3 r_3$, les relations précédentes deviennent

$$\overrightarrow{s} = (\overrightarrow{p} \cdot \overrightarrow{r})\overrightarrow{p},$$

et donc

$$\|\overrightarrow{s}\|^2 = (\overrightarrow{p} \cdot \overrightarrow{r})^2. \tag{2.3.16}$$

Toujours en utilisant le système 2.3.15, on peut calculer $\overrightarrow{s}$:

$$\overrightarrow{s} \cdot \overrightarrow{r} = s_1 r_1 + s_2 r_2 + s_3 r_3 = (\overrightarrow{p} \cdot \overrightarrow{r})^2. \tag{2.3.17}$$

En combinant les équations 2.3.16 et 2.3.17, on trouve que

$$\|\overrightarrow{s}\|^2 = \overrightarrow{s} \cdot \overrightarrow{r}. \tag{2.3.18}$$

C'est en effet une condition *nécessaire* pour que ρ' soit le résultat d'une mesure de projection sur ρ. Pour prouver la suffisance, il suffit de montrer que le système 2.3.15 admet au moins une solution $\overrightarrow{p}$ qui convient. Mais d'après 2.3.16, $\overrightarrow{p} \cdot \overrightarrow{r} = \pm \|\overrightarrow{s}\|$. On choisit donc

$$\overrightarrow{p} = \frac{\overrightarrow{s}}{\|\overrightarrow{s}\|}.$$

3 Sous-additivité forte

Un des résultats les plus profonds sur l'information quantique est sans doute l'inégalité appelée la sous-additivité forte. Elle est aussi un théorème assez difficile : conjecturée en 1968 par Lanford et Robinson, elle a été prouvée en 1973 par Lieb et Ruskai [LR73]. Il faut aussi remarquer que le cas d'égalité n'a été explicité qu'en 2003, dans [PHW03]. La preuve que je donne ici suis les lignes de Nielsen et Petz ([NP05]).

3.1 Énoncé, propriétés

Théorème 3.1 (sous-additivité forte de l'entropie de Von Neumann). *Soit ρ_{ABC} l'état d'un système ABC. Alors*

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC}). \tag{3.1.19}$$

Comme son nom l'indique, cette inégalité est plus forte que la sous-additivité de la proposition 2.16. En effet si on pose $\rho_{ABC} = \rho_{AC} \otimes |b\rangle\langle b|$ (la partie B est dans un état pur et n'est pas intriquée avec la partie AC du système), alors on retrouve la sous-additivité appliquée au système AC.

A partir de la sous-additivité forte on peut déduire une autre inégalité importante (les deux sont en fait équivalentes) :

Proposition 3.2. *Soit ρ_{ABC} l'état d'un système ABC. Alors*

$$S(\rho_A) + S(\rho_B) \leq S(\rho_{AC}) + S(\rho_{BC}). \tag{3.1.20}$$

Preuve. Montrons d'abord que la sous-additivité forte implique l'inégalité ci-dessus. En effet, soit R un système qui purifie ABC. On a

$$S(\rho_{ACR}) + S(\rho_A) \leq S(\rho_{AC}) + S(\rho_{AR}). \tag{3.1.21}$$

Mais, comme $ABCR$ est pur, on a (par la proposition 2.5) $S(\rho_{ACR}) = S(\rho_B)$ et $S(\rho_{AR}) = S(\rho_{BC})$. En remplaçant ces égalités dans 3.1.21, on trouve 3.2. La preuve de la réciproque utilise le même procédé de purification. Soit donc R un système qui purifie ABC. Alors, en appliquant 3.1.20 au système BCR, on trouve

$$S(\rho_R) + S(\rho_B) = S(\rho_{CR}) + S(\rho_{BC}), \tag{3.1.22}$$

qui, en sachant que $S(\rho_R) = S(\rho_{ABC})$ et que $S(\rho_{CR}) = S(\rho_{AB})$, devient 3.1.19. □

3.2 Preuve du théorème

On démontre d'abord une proposition, intéressante en elle-même :

Proposition 3.3 (monotonie de l'entropie relative). *Soient ρ_{AB} et σ_{AB} deux états d'un système composé. Alors l'entropie relative baisse si on "trace" un des sous-systèmes :*

$$S(\rho_{AB}||\sigma_{AB}) \geq S(\rho_A||\ \sigma_A). \tag{3.2.23}$$

Supposons cette proposition vraie et montrons comment on peut en déduire la sous-additivité forte. Soit donc ρ_{ABC} un état quelconque. Par la proposition, on a

$$S(\rho_{ABC}||\ \rho_A \otimes \rho_{BC}) \geq S(\rho_{AB}||\ \rho_A \otimes \rho_B), \tag{3.2.24}$$

qui, en utilisant la proposition 2.15, se réécrit comme

$$S(\rho_A) + S(\rho_{BC}) - S(\rho_{ABC}) \geq S(\rho_A) + S(\rho_B) - S(\rho_{AB}), \tag{3.2.25}$$

où on peut reconnaître l'inégalité 3.1.19.

Reste à montrer la proposition 3.3. Nous allons montrer l'inégalité pour des opérateurs densité qui sont inversibles, puis déduire le cas général par un argument classique de continuité.

Soient donc ρ et σ deux opérateurs densité inversibles. Définissons les opérateurs $\mathcal{L}$ et $\mathcal{R}$ sur l'espace des matrices positives : $\mathcal{L}(X) = \sigma X$ et $\mathcal{R}(X) = X\rho^{-1}$. Remarquons que $\mathcal{L}$ et $\mathcal{R}$ commutent, et notons $\Delta = \mathcal{L}\mathcal{R}$. Pour définir $\log(\Delta)$, il faut montrer d'abord que $\mathcal{L}$, $\mathcal{R}$ et ensuite Δ sont des opérateurs strictement positifs pour le produit scalaire de Hilbert-Schmidt $\langle X, Y\rangle = \mathrm{tr}(X^*Y)$. Pour $\mathcal{L}$ et $\mathcal{R}$ c'est du simple calcul, et pour Δ c'est évident car il s'agit d'un produit d'opérateurs strictement positifs et qui commutent. De même on peut montrer que $\log(\mathcal{L})(X) = \log(\sigma)X$ et que $\log(\mathcal{R})(X) = -X\log(\rho)$. Bien sur, comme $\mathcal{L}$ et $\mathcal{R}$ commutent, $\log(\Delta) = \log(\mathcal{L}) + \log(\mathcal{R})$. On est maintenant en mesure d'exprimer l'entropie relative en utilisant l'opérateur Δ :

$$S(\rho||\sigma) = \langle \rho^{1/2}, -\log(\Delta)(\rho^{1/2})\rangle. \tag{3.2.26}$$

En effet, l'opérateur Δ permet d'avoir un seul "log" dans l'expression précédente. Ensuite, l'inégalité à démontrer s'écrit

$$\langle \rho_A^{1/2}, -\log(\Delta_A)(\rho_A^{1/2})\rangle \leq \langle \rho_{AB}^{1/2}, -\log(\Delta_{AB})(\rho_{AB}^{1/2})\rangle. \tag{3.2.27}$$

La dernière étape de la preuve est de trouver un opérateur $\mathcal{U} : M(A) \to M(AB)$ tel que :

1. $\mathcal{U}^*\Delta_{AB}\mathcal{U} = \Delta_A$,
2. $\mathcal{U}(\rho_A^{1/2}) = \rho_{AB}^{1/2}$,
3. $\mathcal{U}$ est une isométrie $M(A) \to M(AB)$.

La deuxième propriété nous permet de deviner la forme de $\mathcal{U}$:

$$\mathcal{U}(X) = (X\rho_A^{-1/2} \otimes I_B)\rho_{AB}^{1/2}. \tag{3.2.28}$$

Ensuite, il est facile de trouver $\mathcal{U}^*$, en lui demandant que $\langle \mathcal{U}^*(Y), X\rangle = \langle Y, \mathcal{U}(X)\rangle$ pour tous $X \in M(A)$ et $Y \in M(AB)$. On trouve :

$$\mathcal{U}^*(Y) = \mathrm{tr}_B(Y\rho_{AB}^{1/2}(\rho_A^{-1/2} \otimes I_B)). \tag{3.2.29}$$

Pour vérifier les deux autres propriétés ($\mathcal{U}^*\Delta_{AB}\mathcal{U} = \Delta_A$ et $\mathcal{U}^*\mathcal{U} = I_A$) il suffit d'injecter l'expression de $\mathcal{U}^*$ et faire les calculs.

Maintenant qu'on dispose de $\mathcal{U}$, on peut réécrire la conclusion du théorème comme

$$\langle \rho_A^{1/2}, -\log(\mathcal{U}^*\Delta_{AB}\mathcal{U})(\rho_A^{1/2})\rangle \leq \langle \rho_{AB}^{1/2}, -\log(\Delta_{AB})(\rho_{AB}^{1/2})\rangle. \tag{3.2.30}$$

Pour conclure, il nous faut les deux lemmes techniques prouvés dans la section suivante. Par le lemme 3.7 appliqué à la fonction opérateur-convexe $x \mapsto -log(x)$, on a

$$-\log(\mathcal{U}^*\Delta_{AB}\mathcal{U}) \leq -\mathcal{U}^*\log(\Delta_{AB})\mathcal{U}. \tag{3.2.31}$$

Si on injecte cette inégalité dans 3.2.30, on obtient

$$\begin{aligned}\langle \rho_A^{1/2}, -\log(\mathcal{U}^*\Delta_{AB}\mathcal{U})(\rho_A^{1/2})\rangle &\leq \langle \rho_A^{1/2}, -\mathcal{U}^*\log(\Delta_{AB})\mathcal{U}(\rho_A^{1/2})\rangle \\ &= \langle \mathcal{U}(\rho_A^{1/2}), \log(\Delta_{AB})\mathcal{U}(\rho_A^{1/2})\rangle \\ &= \langle \rho_{AB}^{1/2}, -\log(\Delta_{AB})(\rho_{AB}^{1/2})\rangle.\end{aligned}$$

□

3.3 Fonctions opérateur-convexes

Ici on s'interresse à deux résultats techniques qui portent sur les fonctions opérateur-convexes. On introduit sur l'espace des matrices hermitiennes M_n l'ordre usuel : on dit que $X \leq Y$ si la matrice $Y - X$ est positive. On peut maintenant introduire le concept clé de cette partie ;

Définition 3.4 (fonction opérateur-convexe). Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$. On dit que f est opérateur-convexe si pour tout $n \geq 1$, pour tous $X, Y \in M_n$ et pour tout $p \in [0, 1]$ on a

$$f(pX + (1-p)Y) \leq pf(X) + (1-p)f(Y). \tag{3.3.32}$$

Passons maintenant aux trois lemmes utilisés dans la preuve de la sous-additivité forte.

Lemme 3.5. La fonction $x \mapsto 1/x$ est opérateur convexe (sur $\mathbb{R}_+^*$).

Preuve. On doit montrer que pour tous X et Y hermitiennes et strictement positives on a

$$(pX + (1-p)Y)^{-1} \leq pX^{-1} + (1-p)Y^{-1}. \tag{3.3.33}$$

Le cas $X = I$ est trivial, car les deux matrices commutent et le résultat est une conséquence de la convexité usuelle de $x \mapsto 1/x$:

$$(pI + (1-p)Y)^{-1} \leq pI + (1-p)Y^{-1}. \tag{3.3.34}$$

Soient maintenant X et Y hermitiennes et strictement positives quelconques. En remplaçant dans 3.3.34 Y par $X^{-1/2}YX^{-1/2}$, l'inégalité devient

$$(pI + (1-p)X^{-1/2}YX^{-1/2})^{-1} \leq pI + (1-p)(X^{-1/2}YX^{-1/2})^{-1}. \tag{3.3.35}$$

Il est facile à monter que la conjugaison par une matrice quelconque préserve les inégalités matricielles. En conjuguant 3.3.35 par $X^{-1/2}$ on obtient 3.3.33. □

Lemme 3.6. La fonction $x \mapsto -\log x$ est opérateur-convexe (sur $\mathbb{R}_+^*$).

Preuve. On va montrer plutôt l'inégalité avec un logarithme naturel à la place de celui en base 2, parce que pour la fonction $x \mapsto -\ln x$ on a la représentation intégrale

$$-\ln(x) = \int_0^\infty \left(\frac{1}{x+t} - \frac{1}{1+t}\right) dt. \tag{3.3.36}$$

Donc, pour toute matrice hermitienne strictement positive X on a

$$-\ln(X) = \int_0^\infty \left((X+tI)^{-1} - (I+tI)^{-1}\right) dt. \tag{3.3.37}$$

A partir de cette égalité on peut conclure si on arrive à monter que

$$(pX + (1-p)Y + tI)^{-1} \leq p(X+tI)^{-1} + (1-p)(Y+tI)^{-1}. \tag{3.3.38}$$

Mais ceci c'est exactement 3.3.33 appliquée à $X + tI$ et $Y + tI$ (qui sont bien sur hermitiennes et strictement positives). □

Lemme 3.7. Soit f une fonction opérateur-convexe et $U : V \to W$ une isométrie. Alors pour tout opérateur X,

$$f(U^*XU) \leq U^* f(X) U. \tag{3.3.39}$$

Preuve. Supposons que U est surjective. Étant aussi une isométrie, on a le résultat plus fort

$$f(U^*XU) = U^* f(X) U. \tag{3.3.40}$$

Sinon, notons W' l'image de V par U. Soit $P : W \to W'$ la projection sur W' et $Q = I - P$ la projection sur le supplément de W'. Notons aussi f_V, f_W et $f_{W'}$ la fonction f selon qu'on l'applique aux opérateurs sur V, W et respectivement W'.

Remarquons que $PU = U$ et que PU est isométrie surjective $V \to W'$. On a donc

$$f_V(U^*XU) = f_V(U^*P(PXP)PU) = U^* P f_{W'}(PXP) PU. \tag{3.3.41}$$

A partir de cette égalité, on voit que pour conclure il suffit de montrer

$$f_{W'}(PXP) \leq P f_W(X) P. \tag{3.3.42}$$

On peut remarquer que

$$f_{W'}(PXP) = P f_W(PXP) P = P f_W(PXP + QXQ) P, \tag{3.3.43}$$

car $P f_W(QXQ) P = 0$. Introduisons $S = P - Q$. S est auto-adjoint et unitaire : $S^* = S$ et $SS^* = (P-Q)(P-Q) = P - PQ - QP + Q = I$. Un peu de calcul nous montre que $PXP + QXQ = (X + SXS)/2$. En utilisant l'hypothèse (f est opérateur-convexe), on a

$$f_W(PXP + QXQ) \leq (f_W(X) + f_W(SXS))/2. \tag{3.3.44}$$

Mais S est unitaire et auto-adjoint, donc $f_W(SXS) = S f_W(X) S$. On trouve donc

$$f_W(PXP + QXQ) \leq (f_W(X) + S f_W(X) S)/2 = P f_W(X) P + Q f_W(X) Q. \tag{3.3.45}$$

En conjuguant par P cette dernière inégalité et en utilisant 3.3.43 on retrouve 3.3.42 qui permet de conclure. □

4 Applications

4.1 Impossibilité du clonage

Un des principaux résultats qui font la différence entre la théorie de l'information classique et sa contrepartie quantique est le théorème de non-clonage. L'information classique peut être copiée avec une précision aussi grande qu'on veut et autant de fois qu'on veut ; la fonction copier/coller des ordinateurs en est témoin. Il se trouve qu'il est impossible de faire la même chose avec des qubits, au moins dans la plus grande généralité.

En effet, considérons $|\varphi\rangle$ et $|\psi\rangle$ deux états quantiques différents et non-orthogonaux d'un système A. Supposons aussi, par l'absurde, qu'on dispose d'une *photocopieuse* quantique U qui fonctionne de la manière suivante : U est un opérateur unitaire sur l'espace de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_A \otimes \mathcal{H}_E$, et si on le fait agir sur un état $|c\rangle \otimes |b\rangle \otimes |e\rangle$ on retrouve à la sortie deux fois l'état à copier et l'environment modifié $|c\rangle \otimes |c\rangle \otimes |f\rangle$ (on peut voir l'état $|b\rangle$ comme le papier blanc dans la photocopieuse). Pour les deux états de départ on a

$$\begin{aligned} U(|\varphi\rangle \otimes |b\rangle \otimes |e\rangle) &= |\varphi\rangle \otimes |\varphi\rangle \otimes |f\rangle \\ U(|\psi\rangle \otimes |b\rangle \otimes |e\rangle) &= |\psi\rangle \otimes |\psi\rangle \otimes |g\rangle \end{aligned}$$

En prenant le produit scalaire de ces deux relations on trouve

$$\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2 \langle f|g\rangle,$$

et donc, comme $\langle\varphi|\psi\rangle \neq 0$, on a

$$1 = \langle\varphi|\psi\rangle\langle f|g\rangle.$$

Les états étant normalisés, $|\langle f|g\rangle| \leq 1$, et donc $|\langle\varphi|\psi\rangle| = 1$. En utilisant la condition d'égalité dans Cauchy-Schwarz, on en déduit que $|\varphi\rangle$ et $|\psi\rangle$ représentent le même rayon dans $\mathcal{H}_A$, et donc le même état quantique, en contradiction avec les hypothèses de départ.

Évidement, on aurait pu considérer une photocopieuse simplifiée, sans faire apparaître l'environment $\mathcal{H}_E$, mais cela n'aurait rien changé au résultat obtenu. Il est aussi évident qu'on peut imaginer une machine capable de copier deux états $|\varphi\rangle$ et $|\psi\rangle$ orthogonaux, mais qui échoue dès qu'on lui demande de copier un troisième état non-orthogonal à un des deux premiers. Celle-ci serait en quelque sorte une photocopieuse *classique*.

4.2 Codage dense

La notion de codage dense apparaît lorsqu'on dispose d'une voie de communication quantique, c'est à dire un moyen de transmettre un état quantique (d'habitude un ou plusieurs qubits) d'un émetteur à un récepteur. On se demande si l'usage d'une telle voie de communication est "meilleure" que sa contrepartie classique. On peut noter que si on n'utilise que des états quantiques orthogonaux (du style $|0\rangle$ et $|1\rangle$) et des mesures de projection dans les bases respectives, tout ce qu'on peut faire avec une voie classique peut être réalisé avec la voie quantique, en travaillant avec des $|0\rangle$ et des $|1\rangle$ à la place des 0 et des 1. Donc la voie quantique n'est en aucun cas pire. On peut montrer qu'elle est même meilleure, mais avec une hypothèse supplémentaire : les deux parties qui communiquent (qu'on nomme traditionnellement *Alice* et *Bob*) doivent partager une paire de qubits intriqués ; ceci est le but du *codage dense*.

La situation est la suivante : Alice veut communiquer à Bob *deux* bits d'information classique en utilisant *une seule fois* la voie quantique dont ils disposent. Alice et Bob possèdent aussi chacun un qubit d'une paire intriquée qui se trouve (disons) dans l'état de Bell $|\Phi^+\rangle$; ils vont utiliser cette paire, et donc l'intrication, comme une ressource qui va leur permettre de transmettre deux bits en utilisant un seul qubit. Voilà comment ils vont procéder :

1. Alice code les deux bits qu'elle veut transmettre à Bob par un nombre k de 0 à 3.

2. Alice applique la transformation unitaire σ_k à son qubit de la paire $|\Phi^+\rangle$ qu'elle partage avec Bob. Je rappelle que le matrices de Pauli sont notées traditionnellement avec

$$\begin{aligned}\sigma_0 &= I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\\ \sigma_1 &= \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\\ \sigma_2 &= \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix},\\ \sigma_3 &= \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.\end{aligned}$$

3. Après cette transformation, l'état des deux qubits devient (selon la valeur de k) :
   - $k = 0 : |\Phi^+\rangle \to |\Phi^+\rangle$,
   - $k = 1 : |\Phi^+\rangle \to |\Psi^+\rangle$,
   - $k = 2 : |\Phi^+\rangle \to |\Psi^-\rangle$,
   - $k = 3 : |\Phi^+\rangle \to |\Phi^-\rangle$.
4. Alice transmet son qubit à Bob en utilisant la voie quantique.
5. Bob mesure la paire dans la base de projection $(|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle), |\Psi^-\rangle)$, et détermine ainsi la valeur de k choisi par Alice.
6. Bob est maintenant en possession des deux bits d'information classique, et la voie de communication n'a été utilisée qu'une seule fois.

Non seulement ce protocole permet d'envoyer deux bits classiques en utilisant un seul qubit, il est sécurisé dans le sens suivant : si jamais une espionne (nommé traditionnellement Eve) écoute la transmission quantique, elle ne peut rien apprendre sur les bits envoyés. De son point de vue le qubit envoyé se trouve dans l'état

$$\begin{aligned}\rho = p_0 \operatorname{tr}_B(|\Phi^+\rangle\langle\Phi^+|) + p_1 \operatorname{tr}_B(|\Psi^+\rangle\langle\Psi^+|) +\\ +p_2 \operatorname{tr}_B(|\Psi^-\rangle\langle\Psi^-|) + p_3 \operatorname{tr}_B(|\Phi^-\rangle\langle\Phi^-|) = \frac{1}{2}I,\end{aligned}$$

qui ne possède aucune information classique.

4.3 Téléportation quantique

Bien que la téléportation quantique n'a (pour l'instant...) rien à voir avec la téléportation utilisée par les personnages de la célèbre série <Star Trek>, il s'agit d'un procédé utilisé pour transmettre l'état d'une particule à distance sur une particule du même type. La méthode théorique a été découverte en 1992 ; en 1997 trois équipes ont réussi à téléporter des photons. Aujourd'hui il est possible de téléporter des faisceaux laser entiers, et même des atomes (2004).

Examinons en détail le procédé théorique. Deux parties, Alice et Bob veulent n'utiliser que de l'information classique pour communiquer des états (inconnus !) quantiques. Supposons que Alice dispose d'un qubit et que Bob cherche à connaître son état. Même si Alice connaissait les coordonnées de son qubit dans une base, pour les communiquer à Bob il lui faudrait une infinité des bits classiques (il s'agit de deux nombres complexes). Si elle ne connaît pas ces deux nombres il lui est impossible de les trouver sans modifier l'état de son qubit. Quoi faire ?

Comme dans la section précédente, Alice et Bob disposent d'une ressource précieuse : une paire de qubits intriqués dans l'état $|\Phi^+_{AB}\rangle$. Voilà comme ils procèdent :

1. Alice met à côté le qubit à téléporter $|\psi_C\rangle = a|0_C\rangle + b|1_C\rangle$ avec son qubit de la paire $|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$. L'état du système devient

$$|\psi_C\rangle \otimes |\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}\left(a|0_C 0_A 0_B\rangle + a|0_C 1_A 1_B\rangle + b|1_C 0_A 0_B\rangle + b|1_C 1_A 1_B\rangle\right),$$

   qu'on peut réécrire (après calcul) comme

$$\frac{1}{2}|\Phi^+_{CA}\rangle \otimes |\psi_B\rangle + \frac{1}{2}|\Psi^+_{CA}\rangle \otimes \sigma_1|\psi_B\rangle + \frac{1}{2}|\Psi^-_{CA}\rangle \otimes (i\sigma_2)|\psi_B\rangle + \frac{1}{2}|\Phi^-_{CA}\rangle \otimes \sigma_3|\psi_B\rangle.$$

2. Ensuite elle mesure ces deux qubits dans la base $(|\Phi^+_{CA}\rangle, |\Phi^-_{CA}\rangle, |\Psi^+_{CA}\rangle), |\Psi^-_{CA}\rangle)$.
3. Elle obtient deux bits classiques d'information (car il y a 4 résultats possibles de sa mesure) qu'elle envoie à Bob. On remarque que d'après la dernière formule, les 4 résultats sont équiprobables, donc le message envoyé est complètement aléatoire. Alice et Bob n'obtiennent de cette façon aucune information sur le qubit envoyé.
4. Bob connaît donc l'état des qubits d'Alice (car il vient de recevoir par la voie classique le résultat de sa mesure). Il applique une opération à son qubit $|\cdot_B\rangle$, selon le schéma suivant :
   - $|\Phi^+_{CA}\rangle \to \sigma_0$,
   - $|\Psi^+_{CA}\rangle \to \sigma_1$,
   - $|\Psi^-_{CA}\rangle \to \sigma_2$,
   - $|\Phi^-_{CA}\rangle \to \sigma_3$.
5. Ceci transforme son qubit $|\cdot_B\rangle$ dans une copie parfaite de $|\psi_C\rangle$.

Pour finir, remarquons que ce procédé n'entre pas en contradiction avec le théorème de non-clonage, car même si le qubit de Bob est une copie parfaite du qubit initial d'Alice, celui d'Alice est détruit pendant le processus (plus précisément par la mesure d'Alice).

5 Appendice 1 : Rappels de théorie de l'information classique

L'introduction et le développement de l'entropie (classique) par Claude Shannon ont marqué la naissance d'une nouvelle discipline, la théorie de l'information. Dans cette section, on va introduire les idées de base de cette théorie qui vont servir comme modèle pour leurs contreparties quantiques. Les références classiques pour la théorie de l'information sont [CT91] et [Gra90].

Définition 5.1 (entropie de Shannon). Soit X une variable aléatoire discrète et $p(x) = P(X = x)$ sa distribution de probabilité. On définit l'entropie de Shannon de X (ou de $(p(x))_x$) par l'égalité

$$H(X) = H(p(x)) = -\sum_x p(x)\log p(x). \tag{5.0.46}$$

Remarque 5.2. L'entropie de X ne dépend pas des valeurs que la variable aléatoire X prend, mais seulement de sa distribution de probabilités $(p(x))_x$. C'est pour cette raison qu'on parle parfois de l'entropie d'une distribution de probabilités. Ici, et dans toute la suite, on fait la convention $0\log 0 = 0$, justifiée par le prolongement par continuité en 0 de la fonction $x \mapsto x\log x$.

Remarque 5.3. De la même manière, on peut définir l'entropie jointe d'un couple (X, Y) de variables aléatoires :

$$H(X,Y) = H(p(x,y)) = -\sum_{x,y} p(x,y)\log p(x,y). \tag{5.0.47}$$

Définition 5.4 (entropie conditionnelle).

$$H(X|Y) = H(X,Y) - H(X). \tag{5.0.48}$$

Remarque 5.5. En explicitant en fonction de la distribution de probabilités du couple (X,Y), on a

$$H(X|Y) = -\sum_{x,y} p(x,y) \log p(x|y) = \sum_y p(y) H(X|Y=y).$$

Corollaire 5.6 (positivité de l'entropie conditionnelle).

$$H(X|Y) \geq 0, \tag{5.0.49}$$

avec égalité si et seulement si Y est une fonction de X, $Y = f(X)$. En particulier, on a

$$H(X) \leq H(X,Y). \tag{5.0.50}$$

Définition 5.7 (entropie relative).

$$H(p\|q) = \sum_x p(x) \log \frac{p(x)}{q(x)}$$

Le lemme suivant est très important, car il est à la base des résultats qui suivent :

Lemme 5.8. Soient $a_1, \dots a_n, b_1, \dots b_n$ des nombres positives. Alors

$$\sum_{i=1}^n a_i \log \frac{a_i}{b_i} \geq \left(\sum_{i=1}^n a_i \right) \log \frac{\sum_{i=1}^n a_i}{\sum_{i=1}^n b_i} \tag{5.0.51}$$

Proposition 5.9 (positivité de l'entropie relative). *Soient $p(x)$ et $q(x)$ deux distributions de probabilités. Alors*

$$H(p\|q) \geq 0, \tag{5.0.52}$$

avec égalité si et seulement si $p(x) = q(x)$ pour tout x.

Proposition 5.10 (valeur maximale de l'entropie). *Soit d le cardinal de l'image de X. Alors*

$$H(X) \leq \log d, \tag{5.0.53}$$

avec égalité si et seulement si la distribution de X est uniforme.

Proposition 5.11 (sous-additivité).

$$H(X,Y) \leq H(X) + H(Y), \tag{5.0.54}$$

avec égalité si et seulement si X et Y sont indépendantes.

Proposition 5.12 (convexité de l'entropie relative). *La fonction entropie relative $(p,q) \mapsto H(p\|q)$ est convexe en (p,q), i.e. si (p_1,q_1) et (p_2,q_2) sont deux paires de distributions de probabilités, alors*

$$H(\lambda p_1 + (1-\lambda)p_2 \| \lambda q_1 + (1-\lambda)q_2) \leq \lambda H(p_1\|q_1) + (1-\lambda) H(p_2\|q_2), \tag{5.0.55}$$

pour tout $0 \leq \lambda \leq 1$.

Proposition 5.13 (sous-additivité forte).

$$H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z). \tag{5.0.56}$$

6 Appendice 2 : Rappels de théorie quantique

Ces rappels s'adressent à un public mathématique et présentent les notions de base de mécanique quantique. On met l'accent surtout sur les notions utilisées dans ce mémoire. On ne s'intéresse qu'aux systèmes avec un nombre fini de degrés de liberté, donc on va travailler avec des espaces de dimension finie.

6.1 États quantiques, premier formalisme

Un système quantique avec n degrés de liberté sera décrit par un *espace de Hilbert* de dimension n, noté $\mathcal{H}$. On choisit une base orthonormale $\{|e_1\rangle, |e_2\rangle, \ldots, |e_n\rangle\}$, et on appelle les vecteurs $|e_i\rangle$ *vecteurs de base*. Un *état* du système est un vecteur de longueur 1 de $\mathcal{H}$, à une constante de module 1 près. Donc les vecteurs $|x\rangle$ et $|y\rangle = e^{i\theta}|x\rangle$ correspondent à un même état quantique. Les états autres que les vecteurs de base seront appelés *états superposés*.

Soient maintenant deux systèmes non-identiques A et B décrits par les espaces de Hilbert $\mathcal{H}_A$ et $\mathcal{H}_B$. Le système composé AB est alors décrit par l'espace *produit tensoriel* $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Un état $|z\rangle$ du système AB est dit *décomposable* s'il existe des états $|x\rangle \in \mathcal{H}_A$ et $|y\rangle \in \mathcal{H}_B$ tels que $|z\rangle = |x\rangle \otimes |y\rangle$. Sinon, $|z\rangle$ est appelé *intriqué*.

D'habitude on travaille avec des systèmes à deux niveaux, appelés des *qubits*. La base usuelle dans ce cas est notée traditionnellement $\{|0\rangle, |1\rangle\}$. Pour les systèmes formés de k qubits, on travaille dans la base usuelle $\{|00\cdots00\rangle$, $|00\cdots01\rangle$, …, $|11\cdots11\rangle\}$. Introduisons maintenant quatre états quantiques très importants par la suite :

Définition 6.1 (états de Bell).
- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$,
- $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$,
- $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

Comment évoluent les systèmes quantiques dans le temps ? S'il existe une telle évolution alors il existe des fonctions $U_t : \mathcal{H} \to \mathcal{H}$ qui dépendent du temps t et telles que

$$|x_t\rangle = U_t|x_0\rangle. \tag{6.1.57}$$

Ces fonctions U_t vérifient quatre propriétés naturelles :

1. Les U_t doivent transformer vecteurs états en vecteurs états, donc elles doivent *préserver la norme* :
$$\forall t \in \mathbb{R}, \forall x \in \mathcal{H} \ \|U_t x\| = \|x\|. \tag{6.1.58}$$
2. Pour tout temps t, la fonction U_t est *linéaire*.
3. La *loi du groupe* :
$$\forall t, t' \in \mathbb{R}, U_{t+t'} = U_t U_{t'}. \tag{6.1.59}$$
4. La *continuité* :
$$\forall t_0 \in \mathbb{R}, \lim_{t\to t_0} U_t|x_0\rangle = \lim_{t\to t_0} |x_t\rangle = |x_{t_0}\rangle. \tag{6.1.60}$$

Le théorème suivant, dû à Stone (voir [Par92]), donne la structure des U_t :

Théorème 6.2. *Soit $(U_t)_{t\in\mathbb{R}}$ une famille d'opérateurs qui vérifient les conditions 1-4 ci-dessus. Alors il existe un unique opérateur auto-adjoint H tel que*
$$\forall t \in \mathbb{R}, U_t = e^{-itH}. \tag{6.1.61}$$

En dérivant l'équation 6.1.61, on obtient la fameuse équation de Schrödinger :

$$i\frac{\mathrm{d}}{\mathrm{dt}}|x_t\rangle = H|x_t\rangle. \tag{6.1.62}$$

Pour finir la description de ce premier formalisme, on va introduire les mesures quantiques, les *observables*. A toute propriété physique mesurable on associe un opérateur hermitien

$$A = a_1P_1 + a_2P_2 + \ldots + a_kP_k, \tag{6.1.63}$$

appelé une observable. Dans l'équation 6.1.63, les a_i sont les valeurs propres distinctes de A et représentent les *résultats possibles* de la mesure. En fait, les mesures quantiques sont probabilistes, et on obtient le résultat a_i avec la probabilité

$$P(a_i) = \langle x|P_ix\rangle, \tag{6.1.64}$$

sachant que l'état du système au moment de la mesure est $|x\rangle$. Ensuite (si on obtient le résultat a_i), l'état du système devient

$$|x_i'\rangle = \frac{P_i|x\rangle}{\|P_i|x\rangle\|}. \tag{6.1.65}$$

6.2 États quantiques, deuxième formalisme

Comme on peut le voir facilement, les quatre états de Bell (définition 6.1) sont intriqués, i.e. ils ne peuvent pas s'écrire comme un produit tensoriel. Quel sens peut-on donner à une partie de ce système de 2 qubits ? Le deuxième formalisme qu'on va introduire va répondre à cette question.

A tout état quantique $|x\rangle$ on associe l'opérateur $|x\rangle\langle x|$ appelé *opérateur densité* ou encore matrice densité. Il est facile de voir que $|x\rangle\langle x|$ est auto-adjoint, positif et de trace unité. En utilisant ces propriétés, on généralise la notion d'état quantique :

Définition 6.3 (opérateur densité, état d'un système). L'état d'un système quantique est un opérateur hermitien, positif et de trace unité dans $\mathcal{H}$, appelé opérateur densité.

Étant auto-adjoint, un opérateur densité ρ admet la *décomposition spectrale*

$$\rho = \lambda_1|x_1\rangle\langle x_1| + \lambda_2|x_2\rangle\langle x_2| + \ldots + \lambda_n|x_n\rangle\langle x_n|. \tag{6.2.66}$$

Si tous les λ_i sont nuls sauf un seul qui vaut 1, alors ρ est de la forme $|x\rangle\langle x|$ et il est appelé un *état pur*. Sinon, ρ est dit *mélangé*.

Comme dans le premier formalisme, si un système A se trouve dans un état ρ_A et un système B dans un état ρ_B, alors le système AB se trouve dans l'état produit tensoriel $\rho_{AB} = \rho_A \otimes \rho_B$. Pour répondre à la question du début, on introduit la notion de trace partielle :

Définition 6.4 (trace partielle, état d'un sous-système). Soit AB un système composé qui se trouve dans un état ρ_{AB}. Alors les sous-systèmes A et B se trouvent dans les états ρ_A respectivement ρ_B tels que pour tout X opérateur auto-adjoint sur $\mathcal{H}_A$ et pour tout Y opérateur auto-adjoint sur $\mathcal{H}_B$, on ait :

$$\mathrm{tr}(\rho_AX) = \mathrm{tr}(\rho_{AB}(X \otimes I_B)), \tag{6.2.67}$$

$$\mathrm{tr}(\rho_BY) = \mathrm{tr}(\rho_{AB}(I_A \otimes Y)). \tag{6.2.68}$$

On note

$$\rho_A = \mathrm{tr}_B(\rho_{AB}), \tag{6.2.69}$$

et

$$\rho_B = \mathrm{tr}_A(\rho_{AB}). \tag{6.2.70}$$

Pour traduire l'évolution temporelle et les mesures introduites dans la section précédente dans ce formalisme, il suffit juste de généraliser les définitions pour des états purs. En ce qui concerne l'évolution unitaire, on obtient

$$\rho(t) = U(t)\rho(0)U(t)^*, \tag{6.2.71}$$

qui peut s'écrire comme l'équation de Schrödinger généralisée ($[X, Y] = XY - YX$ est appelé le *commutateur* de X et Y) :

$$i\frac{\mathrm{d}}{\mathrm{dt}}\rho(t) = [H, \rho(t)]. \tag{6.2.72}$$

Enfin, si on mesure une observable

$$A = a_1P_1 + a_2P_2 + \ldots + a_kP_k, \tag{6.2.73}$$

sur un état ρ, on trouve la réponse a_i avec la probabilité

$$P(a_i) = \mathrm{tr}(P_i\rho). \tag{6.2.74}$$

Enfin, si on mesure l'observable A, mais on ignore le résultat obtenu, l'état du système devient

$$\rho' = \sum_{i=1}^{k} P_i\rho P_i. \tag{6.2.75}$$

6.3 Décomposition de Schmidt et purification quantique

Un des outils les plus puissants utilisés dans la théorie de l'information quantique est la purification. C'est un procédé qui permet d'écrire tout opérateur densité comme la trace partielle d'un état pur qui vit dans un espace plus grand. Avant d'énoncer et prouver ce résultat, regardons une proposition importante et très utile :

Proposition 6.5 (décomposition de Schmidt). *Soient A et B deux systèmes de dimensions n et m avec $n \leq m$. Soit $|z\rangle$ un état pur du système composé AB et ρ_A et ρ_B les états des systèmes A et B. Soit*

$$\rho_A = \lambda_1|x_1\rangle\langle x_1| + \ldots + \lambda_n|x_n\rangle\langle x_n| \tag{6.3.76}$$

une décomposition spectrale de ρ_A. Alors

$$|z\rangle = \sqrt{\lambda_1}|x_1\rangle \otimes |y_1\rangle + \ldots + \sqrt{\lambda_n}|x_n\rangle \otimes |y_n\rangle, \tag{6.3.77}$$

où $\{y_i|\lambda_i \neq 0\}$ est un ensemble orthonormal (pas forcement une base) de vecteurs propres de ρ_B.

Preuve. Soit $\{|b_1\rangle, \ldots, |b_m\rangle\}$ une base orthonormale de $\mathcal{H}_B$. Alors $|z\rangle$ s'écrit

$$|z\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}|x_i\rangle \otimes |b_j\rangle = \sum_{i=1}^{n} |x_i\rangle \otimes |y_i'\rangle = \sum_{j=1}^{m} |x_j'\rangle \otimes |b_j\rangle, \tag{6.3.78}$$

où

$$y'_i = \sum_{j=1}^{m} c_{ij} b_j \tag{6.3.79}$$

et

$$x'_j = \sum_{i=1}^{n} c_{ij} x_i. \tag{6.3.80}$$

A partir de la deuxième égalité de 6.3.78, on écrit

$$\rho_A = \mathrm{tr}_B(|z\rangle\langle z|) = \sum_{k=1}^{m} |x'_k\rangle\langle x'_k| = \sum_{k=1}^{m} |\sum_{i=1}^{n} c_{ik} x_i\rangle\langle \sum_{j=1}^{n} c_{jk} x_j| = \sum_{k=1}^{m}\sum_{i=1}^{n}\sum_{j=1}^{n} c_{ik} c^*_{jk} |x_i\rangle\langle x_j|. \tag{6.3.81}$$

Mais on a aussi

$$\langle y'_j|y'_i\rangle = \langle \sum_{k=1}^{m} c_{jk} b_k| \sum_{l=1}^{m} c_{il} b_l\rangle = \sum_{k=1}^{m}\sum_{l=1}^{m} c^*_{jk} c_{il} \langle b_k|b_l\rangle = \sum_{k=1}^{m} c^*_{jk} c_{ik}, \tag{6.3.82}$$

et donc ρ_A s'écrit comme

$$\rho_A = \sum_{i=1}^{n}\sum_{j=1}^{n} \langle y'_j|y'_i\rangle |x_i\rangle\langle x_j|. \tag{6.3.83}$$

En comparant 6.3.76 et 6.3.83, on en déduit que

$$\langle y'_j|y'_i\rangle = \begin{cases} \lambda_i & \text{, si } j = i \\ 0 & \text{, sinon.} \end{cases} \tag{6.3.84}$$

Pour conclure, posons $|y'_i\rangle = \sqrt{\lambda_i}|y_i\rangle$. On trouve

$$|z\rangle = \sqrt{\lambda_1}|x_1\rangle \otimes |y_1\rangle + \ldots + \sqrt{\lambda_n}|x_n\rangle \otimes |y_n\rangle \tag{6.3.85}$$

et

$$\rho_B = \lambda_1 |y_1\rangle\langle y_1| + \ldots + \lambda_n |y_n\rangle\langle y_n|. \tag{6.3.86}$$

□

Proposition 6.6 (purification quantique). *Soit ρ l'état d'un système quantique A. Alors il existe un autre système B et $|z\rangle$ un état pur sur $\mathcal{H}_A \otimes \mathcal{H}_B$ tel que $\rho = \mathrm{tr}_B(|z\rangle\langle z|)$.*

Preuve. Considérons la décomposition spectrale de ρ :

$$\rho = \lambda_1 |x_1\rangle\langle x_1| + \ldots + \lambda_n |x_n\rangle\langle x_n|. \tag{6.3.87}$$

D'après la preuve de la proposition précédente, il suffit de choisir $\mathcal{H}_B = \mathcal{H}_A$ et de poser

$$|z\rangle = \sqrt{\lambda_1}|x_1\rangle \otimes |y_1\rangle + \ldots + \sqrt{\lambda_n}|x_n\rangle \otimes |y_n\rangle, \tag{6.3.88}$$

où les y_i forment une base orthonormale quelconque de $\mathcal{H}_B$. □

Références

[CT91] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley and Sons, 1991.

[Gra90] Robert M. Gray. *Entropy and Information Theory*. Springer, 1990.

[Gru99] Josef Gruska. *Quantum Computing*. McGraw-Hill, 1999.

[Hir04] Mika Hirvensalo. *Quantum Computing*. Springer, 2004.

[LR73] E. H. Lieb and M. B. Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. *J. Math. Phys, 14 :1938-1941*, 1973.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NP05] Michael A. Nielsen and Dénes Petz. A simple proof of the simple subadditivity inequality. *arXiv :quant-ph/0408130*, 2005.

[Par92] K.R. Parthasarathy. *An introduction to quantum stochastic calculus*. Birkhäuser, 1992.

[PHW03] Dénes Petz Patrick Hayden, Richard Jozsa and Andreas Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *arXiv :quant-ph/0304007*, 2003.

[Pre98] John Preskill. Quantum information and computation. Technical report, California Institute of Technology, September, 1998.