Introduction au Calcul Quantique

3. L'état à plusieurs qubits

Edouard Marchais[a]

[a] *EPITA, 14-16 Rue Voltaire, 94270 Le Kremlin-Bicêtre, France.*

E-mail: edouard.marchais@epita.fr

Abstract: La notion d'état quantique de systèmes composés est discuté en détail en précisant leur structure mathématique inhérente. Le concept central de produit tensoriel est mis en avant afin d'expliquer la possibilité d'état intriqué aux propriétés physiques différentes d'un état pur jusque là considéré. Le théorème de non clonage d'un état quantique est également analyser à travers un exemple. Enfin une illustration de l'utilisation des états à plusieurs qubits est fourni à travers l'exemple de la téléportation quantique.

Table des Matières

1 États à deux qubits

Introduction On pourrait s'attendre à ce que le passage d'un qubit à deux qubits n'apporte que peu de nouveauté. En fait nous allons voir que la structure à deux qubits est extraordinairement riche, car elle introduit des *corrélations quantiques* entre les deux qubits, et on ne peut pas en rendre compte par des considérations de probabilités classiques. Comme nous le verrons, ces configurations de systèmes quantiques, dites intriquées, sont à la base des spécificités du *calcul quantique*. En revanche, le passage de deux qubits à n qubits n'apporte aucune nouveauté de principe.

Exemple simple La construction mathématique d'un état à deux qubits repose sur la notion de *produit tensoriel*, notion que nous allons introduire sur un exemple élémentaire. Soit $\mathcal{H}_A$ un espace vectoriel de fonctions $f_A(x)$ à deux dimensions, par exemple de vecteurs de base $\{\cos x, \sin x\}$, alors

$$f_A(x) = \lambda_A \cos x + \mu_A \sin x$$

et $\mathcal{H}_A$ un autre espace vectoriel de fonctions $f_B(y)$ à deux dimensions avec pour vecteurs de base $\{\cos y, \sin y\}$, alors

$$f_B(y) = \lambda_B \cos y + \mu_B \sin y$$

On peut former la fonction de deux variables « produit tensoriel de f_A et f_B »

$$f_A(x) f_B(x) = \lambda_A\lambda_B \cos x \cos y + \lambda_A\mu_B \cos x \sin y + \mu_A\lambda_B \sin x \cos y + \mu_A\mu_B \sin x \sin y$$

Une base possible de l'espace produit tensoriel est

$$\{\cos x \cos y, \cos x \sin y, \sin x \cos y, \sin x \sin y\}$$

Toute fonction de cet espace peut se décomposer suivant cette base

$$g(x, y) = \alpha \cos x \cos y + \beta \cos x \sin y + \gamma \sin x \cos y + \delta \sin x \sin y$$

mais cette fonction n'est pas en général de la forme produit tensoriel, $f_A(x)\, f_B(y)$! Une condition *nécessaire (et suffisante)* est que $\alpha\delta = \beta\gamma$.

Construction du produit tensoriel Nous allons suivre le schéma ci-dessus pour construire mathématiquement un état à deux qubits. Le premier qubit A, vit dans un espace de Hilbert $\mathcal{H}_A$, dont une base orthonormée est $\{|0_A\rangle, |1_A\rangle\}$, et le second qubit B dans un espace de Hilbert $\mathcal{H}_B$ dont une base orthonormée est $\{|0_B\rangle, |1_B\rangle\}$. Il est naturel de représenter un état physique où le premier qubit est dans l'état $|0_A\rangle$ et le second dans l'état $|0_B\rangle$ par un vecteur que l'on écrit $|X_{00}\rangle = |0_A \otimes 0_B\rangle$; en prenant en compte les autres valeurs possibles de qubits on aura à priori quatre possibilités

$$|X_{00}\rangle = |0_A\rangle \otimes |0_B\rangle \qquad |X_{01}\rangle = |0_A\rangle \otimes |1_B\rangle \qquad |X_{10}\rangle = |1_A\rangle \otimes |0_B\rangle \qquad |X_{11}\rangle = |1_A\rangle \otimes |1_B\rangle$$

La notation $\otimes$ désigne le produit tensoriel. Il n'est pas difficile de construire l'état où le qubit A est dans

$$|\varphi_A\rangle = \lambda_A|0_A\rangle + \mu_A|1_A\rangle$$

et le qubit B dans

$$|\varphi_B\rangle = \lambda_B|0_B\rangle + \mu_B|1_B\rangle$$

On notera cet état $|\varphi_A \otimes \varphi_B\rangle$ et

$$\begin{aligned}|\varphi_A \otimes \varphi_B\rangle &= \lambda_A\lambda_B|0_A\rangle \otimes |0_B\rangle + \lambda_A\mu_B|0_A\rangle \otimes |1_B\rangle + \mu_A\lambda_B|1_A\rangle \otimes |0_B\rangle + \mu_A\mu_B|1_A\rangle \otimes |1_B\rangle \\ &= \lambda_A\lambda_B|X_{00}\rangle + \lambda_A\mu_B|X_{01}\rangle + \mu_A\lambda_B|X_{10}\rangle + \mu_A\mu_B|X_{11}\rangle\end{aligned}$$

Nous avons construit l'espace $\mathcal{H}_A \otimes \mathcal{H}_B$ produit tensoriel des espaces $\mathcal{H}_A$ et $\mathcal{H}_B$. On note que le vecteur $|\varphi_A \otimes \varphi_B\rangle$ est bien de norme unité[1]. Les physiciens sont assez laxistes sur les notations, et on trouvera au lieu de $|\varphi_A \otimes \varphi_B\rangle$, soit $|\varphi_A\rangle \otimes |\varphi_B\rangle$ soit meme $|\varphi_A\varphi_B\rangle$ en omettant le symbole du produit tensoriel.

Remarque importante *Le point crucial est que l'état le plus general de $\mathcal{H}_A \otimes \mathcal{H}_B$ n 'est pas de la forme produit tensoriel $|\varphi_A \otimes \varphi_B\rangle$* : les états de la forme $|\varphi_A \otimes \varphi_B\rangle$ ne forment qu'un petit sous-ensemble (et pas un sous-espace!) des vecteurs de $\mathcal{H}_A \otimes \mathcal{H}_B$. L'état le plus general est de la forme

$$\begin{aligned}|\Psi\rangle &= \alpha_{00}|0_A \otimes 0_B\rangle + \alpha_{01}|0_A \otimes 1_B\rangle + \alpha_{10}|1_A \otimes 0_B\rangle + \alpha_{11}|1_A \otimes 1_B\rangle \\ &= \alpha_{00}|X_{00}\rangle + \alpha_{01}|X_{01}\rangle + \alpha_{10}|X_{10}\rangle + \alpha_{11}|X_{11}\rangle\end{aligned}$$

et pour que $|\Psi\rangle$ soit de la forme $|\varphi_A \otimes \varphi_B\rangle$, une condition nécessaire (et suffisante) est que

$$\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$$

ce qui n'a aucune raison d'être vrai a priori. Donnons un exemple très simple d'un état $|\Phi\rangle$ qui n'est pas de la forme $|\varphi_A \otimes \varphi_B\rangle$

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\big(|0_A \otimes 1_B\rangle + |1_A \otimes 0_B\rangle\big) \tag{1.1}$$

En effet

$$\alpha_{00} = \alpha_{11} = 0 \qquad \text{et} \qquad \alpha_{01} = \alpha_{10} = \frac{1}{\sqrt{2}} \qquad \text{et} \qquad \alpha_{00}\alpha_{11} \neq \alpha_{01}\alpha_{10}$$

Produit tensoriel d'opérateurs On définit de même le produit tensoriel $\mathcal{M}_A \otimes \mathcal{M}_A$ de deux opérateurs $\mathcal{M}_A$ et $\mathcal{M}_B$

$$[\mathcal{M}_A \otimes \mathcal{M}_A]_{i_A\, p_B; j_A\, q_B} = [\mathcal{M}_A]_{i_A; j_A}\, [\mathcal{M}_A]_{p_B; q_B}$$

Donnons comme exemple le produit tensoriel de deux matrices 2×2

$$\mathcal{M}_A = \begin{pmatrix} a & \mathrm{B} \\ c & d \end{pmatrix} \qquad \text{et} \qquad \mathcal{M}_B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

La matrice $\mathcal{M}_A \otimes \mathcal{M}_B$ est une matrice 4×4, l'ordre de lignes et des colonnes étant $00, 01, 10, 11$

$$\mathcal{M}_A \otimes \mathcal{M}_B = \begin{pmatrix} a\,\mathcal{M}_B & b\,\mathcal{M}_B \\ c\,\mathcal{M}_B & d\,\mathcal{M}_B \end{pmatrix} = \begin{pmatrix} a\,\alpha & \mathrm{A}\,\beta & b\,\alpha & b\,\beta \\ a\,\gamma & \mathrm{A}\,\delta & b\,\gamma & b\,\delta \\ c\,\alpha & \mathrm{C}\,\beta & d\,\alpha & d\,\beta \\ c\,\gamma & \mathrm{C}\,\delta & d\,\gamma & d\,\delta \end{pmatrix}$$

Un état de deux qubits qui n'est pas de la forme $|\varphi_A \otimes \varphi_B\rangle$ est appelé *état intriqué* (en anglais « *entangled state* »). La propriété fondamentale est la suivante : si $|\Psi\rangle$ est un état intriqué, alors le qubit A ne peut pas être dans un état quantique défini $|\varphi_A\rangle$.

[1] En toute rigueur it faudrait verifier que le produit $|\varphi_A \otimes \varphi_B\rangle$ est indépendant du choix des bases dans $\mathcal{H}_A$ et $\mathcal{H}_B$. Cette vérification est immediate.

Valeur moyenne Montrons-le d'abord sur un cas particulier, celui de l'état $|\Phi\rangle$ (1.1). Soit $\mathcal{M}$ une propriété physique du qubit A. Dans l'espace $\mathcal{H}_A \otimes \mathcal{H}_B$ cette propriété physique est représentée par $\mathcal{M} \otimes \mathcal{I}_B$. Calculons sa valeur moyenne $\langle \Phi | \mathcal{M}\Psi \rangle = \langle \mathcal{M} \rangle_\Phi$

$$\begin{aligned} \langle \mathcal{M} \rangle_\Phi &= \frac{1}{2} \big[\langle 0_A \otimes 1_B | + \langle 1_A \otimes 0_B | \big] \big[|(\mathcal{M}\, 0_A) \otimes 1_B \rangle + (\mathcal{M}\, 1_A) \otimes 1_A \rangle \big] \\ &= \frac{1}{2} \big(\langle 0_A | \mathcal{M}\, 0_A \rangle + \langle 1_A | \mathcal{M}\, 1_A \rangle \big) \end{aligned} \tag{1.2}$$

où nous avons utilisé

$$\langle 0_B | 0_B \rangle = \langle 1_B | 1_B \rangle = 1 \qquad \text{et} \qquad \langle 0_B | 1_B \rangle = \langle 1_B | 0_B \rangle = 0$$

Il n'existe pas d'état

$$|\varphi_A\rangle = \lambda\, |0_A\rangle + \mu\, |1_A\rangle$$

tel que

$$\langle \Phi | \mathcal{M}\Psi \rangle = \langle \varphi_A | \mathcal{M}\, \varphi_A \rangle$$

En effet on aurait alors

$$\langle \varphi_A | \mathcal{M}\, \varphi_A \rangle = |\lambda|^2\, \langle 0_A | \mathcal{M}\, 0_A \rangle + \big(\overline{\lambda}\mu\, \langle 0_A | \mathcal{M}\, 1_A \rangle + \lambda \overline{\mu}\, \langle 1_A | \mathcal{M}\, 0_A \rangle \big) + |\mu|^2\, \langle 1_A | \mathcal{M}\, 0_A \rangle$$

Pour reproduire (1.2), une condition nécessaire serait que $|\lambda| = |\mu| = 1/\sqrt{2}$, et les termes en $\overline{\lambda}\mu$ ne seraient pas nuls. Le résultat (1.2) a une interprétation physique simple : l'état du qubit A est un mélange incohérent de 50% de l'état $|0_A\rangle$ et de 50% de l'état $|1_A\rangle$, et non une superposition linéaire. En résumé, on ne peut pas en général décrire une partie d'un système quantique intriqué par un vecteur d'état.

Polarisation Un exemple de mélange incohérent est fourni par la lumière naturelle, non polarisée : c'est un mélange incohérent de 50% de lumière polarisée suivant Ox et de 50% de lumière polarisée suivant Oy alors qu'une lumière polarisée à 45° est une superposition cohérente de 50% de lumière polarisée suivant Ox et de 50 % de lumière polarisée suivant Oy.

$$|\theta = \pi/4\rangle = \frac{1}{\sqrt{2}} \big(|x\rangle + |y\rangle \big)$$

Une lumière polarisée circulairement à droite est aussi une superposition cohérente

$$|D\rangle = \frac{1}{\sqrt{2}} \big(|x\rangle + i\, |y\rangle \big)$$

On voit l'importance des phases : les états $|\theta = \pi/4\rangle$ et $|D\rangle$ par exemple correspondent tous deux à des probabilités de 50% d'observer un photon polarisé suivant Ox ou suivant Oy, mais ces deux états sont complètement différents, l'un est une polarisation linéaire, l'autre une polarisation circulaire.

Résumé Dans cette section nous avons vu comment un état à deux qubits était décrit par un produit tensoriel qui présente une structure *plus riche* que le simple produit des vecteurs d'état. Une conséquence de cette structure tensoriel est la possibilité d'état intriqué qui ne sont pas accessible à une mesure à la valeur moyenne associé à un opérateur hermitien.

2 Opérateur d'état

On va maintenant généraliser ces résultats à un système quantique formé de deux sous-systèmes quelconques, en appelant $|i_A\rangle$ (resp. $|i_B\rangle$) une base orthonormée du sous-système A (resp. B). Afin d'alléger les notations, il sera commode de faire les substitutions $i_A \to i$ et $i_B \to \mu$. L'état le plus général est alors

$$|\Phi\rangle = \sum_{i,\mu} \alpha_{i\mu} \, |i \otimes \mu\rangle$$

Soit $\mathcal{M}$ une propriété physique du sous-système A

$$|\mathcal{M}\Phi\rangle = \sum_{i,\mu} \alpha_{i\mu} \, |\mathcal{M}\, i \otimes \mu\rangle$$

Calculons la valeur moyenne de $\mathcal{M}$

$$\langle\Phi|\mathcal{M}\Phi\rangle = \sum_{i,\nu} \sum_{i,\mu} \overline{\alpha}_{j\nu}\alpha_{i\mu} \, \langle j \otimes \nu|\mathcal{M}\, i \otimes \mu\rangle = \sum_{i,j} \sum_{\mu} \overline{\alpha}_{j\mu}\alpha_{i\mu} \, \langle j|\mathcal{M}\, i\rangle$$

On peut alors sommer sur l'indice μ

$$\langle\Phi|\mathcal{M}\Phi\rangle = \sum_{i,j} \rho_{ij} \, \langle j|\mathcal{M}\, i\rangle = \sum_{i,j} \mathcal{M}_{ji} = \mathrm{Tr}\,(\rho\mathcal{M}) \tag{2.1}$$

Pour obtenir (2.1) égalité on a utilisé

$$\langle j \otimes \mu|\mathcal{M}\, i \otimes \mu\rangle = \delta_{\mu\nu} \, \langle j|\mathcal{M}\, i\rangle$$

car dans $\mathcal{H}_A \otimes \mathcal{H}_B$, $\mathcal{M}$ est en fait $\mathcal{M} \otimes \mathcal{I}_B$. L'équation (2.1) définit un objet qui joue un rôle crucial, l'*opérateur d'état* (ou opérateur densité) ρ du sous-système A

$$\rho_{ij} = \sum_{\mu} \overline{\alpha}_{j\nu}\alpha_{i\mu}$$

L'opérateur d'état du sous-sytème A est aussi appelé *opérateur d'état réduit* et est souvent noté ρ_A. Le sous-système A n'est pas en général décrit par un vecteur d'état, mais par un opérateur d'état. Cet opérateur d'état est hermitien ($\rho = \rho^*$), il est positif[2] ($\rho \geq 0$) et de trace unité : $\mathrm{Tr}\,\rho = 1$

$$\mathrm{Tr}\,\rho = \sum_i \rho_{ii} = \sum_i \sum_\mu |\alpha_{i\mu}|^2 = \|\Phi\|^2 = 1 \tag{2.2}$$

Les états physiques tels que ceux examinés dans précédemment sont appelés des états purs : ils sont décrits par un vecteur d'état. Il est facile de vérifier que l'opérateur d'état d'un état pur obéit à $\rho^2 = \rho$, et inversement tout opérateur d'état tel que $\rho^2 = \rho$ décrit un état pur. Mais la description la plus générale d'un système quantique doit se faire au moyen de l'opérateur d'état.

Comme ρ est hermitien, il peut être diagonalisé et il s'écrit dans une base orthonormée $|i\rangle$ suivant

$$\rho = \sum_i \mathsf{p_i} |\mathsf{i}\rangle\langle\mathsf{i}| \tag{2.3}$$

[2] Un opérateur positif (ou non négatif) A est tel que $\langle\varphi|\mathrm{A}\,\varphi\rangle \geq 0 \, \forall|\varphi\rangle$ (il est strictement positif si $\langle\varphi|\mathrm{A}\,\varphi\rangle > 0$). Il est nécessairement hermitien dans un espace complexe. Une condition nécessaire et suffisante pour qu'un opérateur soit positif est que ses valeurs propres soient non négatives.

En raison de la positivité de ρ, $\mathsf{p_i} \geq 0$ et la condition $\mathrm{Tr}\,\rho = 1$ donne $\sum_i \mathsf{p_i} = 1$, ce qui fait que les $\mathsf{p_i}$ peuvent être interprétés comme des probabilités. On peut dire que ρ représente un mélange statistique (ou simplement mélange) d'états $|i\rangle$, chaque état $|i\rangle$ ayant une probabilité $\mathsf{p_i}$; dans la phase de préparation, chaque état $|i\rangle$ est préparé avec une probabilité $\mathsf{p_i}$, sans cohérence de phase entre les différents états $|i\rangle$.

On peut aisément généraliser (2.2) lorsqu'un système quantique (AB) est décrit par un opérateur d'état ρ_{AB} d'éléments de matrice[3] $\rho^{AB}_{i\mu;j\nu}$, et non un vecteur d'état. Soit $\mathcal{M}$ une propriété physique du système A, qui est donc représentée dans l'espace $\mathcal{H}_A \otimes \mathcal{H}_B$ par l'opérateur hermitien $\mathcal{M} \otimes \mathcal{I}_B$. Nous voudrions trouver un opérateur ρ_A tel que la valeur moyenne de $\mathcal{M}$ soit donnée par

$$\langle \mathcal{M} \rangle = \mathrm{Tr}(\rho_A \mathcal{M}) \tag{2.4}$$

Utilisant le même argument que ci-dessus, nous calculons la valeur moyenne de $\mathcal{M} \otimes \mathcal{I}_B$

$$\langle \mathcal{M} \otimes \mathcal{I}_B \rangle = \mathrm{Tr}\left(\rho_{AB}\left[\mathcal{M} \otimes \mathcal{I}_B\right]\right) = \sum_{i,j,\mu,\nu} \rho^{AB}_{i\mu;j\nu}\, \mathcal{M}_{ij}\, \delta_{\mu\nu} = \sum_{i,j} \mathcal{M}_{ij} \sum_{\mu} \rho^{AB}_{i\mu;j\mu}$$

L'expression généralisant (2.2) montre donc que ρ_A est de la forme

$$\rho^{A}_{ij} = \sum_{\mu} \rho^{AB}_{i\mu;j\nu} \qquad \text{et} \qquad \rho_A = \mathrm{Tr}_B(\rho_{AB}) \tag{2.5}$$

car la valeur moyenne de $\mathcal{M}$ est bien donnée par (2.4) avec le choix (2.5) pour ρ_A. On peut montrer que (2.2) est la solution unique donnant correctement la valeur moyenne de $\mathcal{M}$. L'opération qui permet de passer de ρ_{AB} à ρ_A est appelée la *trace partielle* de ρ_{AB} par rapport à B.

L'importance de la notion d'opérateur d'état est confirmée par le *théorème de Gleason*, que nous énonçons sans démonstration, et qui dit en gros que la description la plus générale d'un système quantique est donnée par un opérateur d'état.

Théorème de Gleason Soit un ensemble de projecteurs $\mathcal{P}_i$ agissant sur l'espace de Hilbert des états $\mathcal{H}$ et soit un test associé à chaque $\mathcal{P}_i$ dont la probabilité de réussite est $\mathsf{p}(\mathcal{P}_\mathsf{i})$ qui vérifie

$$0 \leq \mathsf{p}(\mathcal{P}_\mathsf{i}) \leq 1 \qquad \text{et} \qquad \mathsf{p}(\mathcal{I}) = 1$$

ainsi que

$$\mathsf{p}(\mathcal{P}_\mathsf{i} \cup \mathcal{P}_\mathsf{j}) = \mathsf{p}(\mathcal{P}_\mathsf{i}) + \mathsf{p}(\mathcal{P}_\mathsf{j}) \qquad \text{si} \qquad \mathcal{P}_\mathsf{i} \cap \mathcal{P}_\mathsf{j} = \varnothing \qquad (\text{ou} \;\; \mathcal{P}_\mathsf{i}\mathcal{P}_\mathsf{j} = \delta_{\mathsf{ij}}\mathcal{P}_\mathsf{i})$$

Alors, si la dimension de $\mathcal{H} \geq 3$, il existe un opérateur ρ hermitien, positif et de de trace unité tel que

$$\mathsf{p}(\mathcal{P}_\mathsf{i}) = \mathrm{Tr}(\rho \mathcal{P}_\mathsf{i})$$

En d'autres termes, si l'on veut associer une probabilité $\mathsf{p}(\mathcal{P}_\mathsf{i})$ à un test $\mathcal{P}_i$ avec des propriétés « raisonnables », alors cette probabilité est donnée par une trace impliquant un opérateur d'état.

Il est évident que l'application d'une transformation unitaire à un produit tensoriel de deux qubits redonne un produit tensoriel : si $|\Phi\rangle$ est un produit tensoriel de la forme $|\varphi_A \otimes \varphi_B\rangle$ et si l'on applique sur $|\Phi\rangle$ une transformation unitaire qui est un produit tensoriel de transformations

[3] Afin de rendre la notation plus lisible, AB a été placé en exposant dans l'écriture des éléments de matrice.

agissant sur A et B, $U_A \otimes U_B$, cela correspond simplement à un changement de base orthonormée dans les espaces $\mathcal{H}_A$ et $\mathcal{H}_B$ et on ne peut pas fabriquer d'état intriqué. Pour fabriquer un état intriqué, *il faut faire interagir les deux qubits*. Le théorème de purification de Schmidt, donner sans démonstration, donne une forme générale à ces résultats.

Théorème de purification de Schmidt Tout état $|\Phi\rangle$ de $\mathcal{H}_A \otimes \mathcal{H}_B$ peut s'écrire sous la forme

$$|\Phi\rangle = \sum_j \sqrt{\mathsf{p_i}}\, |i_A \otimes i_B\rangle \qquad \text{avec} \qquad \langle i_A | j_A\rangle = \langle i_B | j_B\rangle = \delta_{ij}$$

Les états $|i_A\rangle$ et $|i_B\rangle$ dépendent bien évidemment de $|\Phi\rangle$. Cette expression donne immédiatement les opérateurs d'état réduits ρ_A et ρ_B. Partons en effet de l'opérateur d'état total ρ_{AB}

$$\rho_{AB} = |\Phi\rangle\langle\Phi| = \sum_{i,j} |i_A \otimes i_B\rangle\langle j_A \otimes j_B|$$

Soit $|i\rangle$ une hase orthonormée de $\mathcal{H}$; il est facile de calculer les traces à l'aide du résultat suivant

$$\mathrm{Tr}|\varphi\rangle\langle\psi| = \sum_i \langle i|\varphi\rangle\langle\psi|i\rangle = \sum_i \langle\varphi|i\rangle\langle i|\psi\rangle = \langle\psi|\varphi\rangle$$

car $\sum_i |i\rangle\langle i| = \mathcal{I}$ et par conséquent, les opérateurs d'état ρ_A et ρ_B sont donnés par

$$\rho_A = \sum_i \mathsf{p_i}\, |\mathsf{i_A}\rangle\langle\mathsf{i_A}| \qquad \text{et} \qquad \rho_\mathsf{B} = \sum_\mathsf{i} \mathsf{p_i}\, |\mathsf{i_B}\rangle\langle\mathsf{i_B}|$$

avec les *mêmes* $\mathsf{p_i}$. Le nombre des $\mathsf{p_i}$ différents de zéro est le *nombre de Schmidt*. Si l'on applique sur un état $|\Phi\rangle$ quelconque une transformation unitaire qui est un produit tensoriel de transformations agissant sur A et B, $U_A \otimes U_B$, on ne peut pas changer le nombre de Schmidt en manipulant séparément les qubits A et B. On retrouve le résultat énoncé ci-dessus pour un produit tensoriel en remarquant que le nombre de Schmidt d'un produit tensoriel est 1. Si $\mathcal{H}_A$ et $\mathcal{H}_B$ sont de dimension N, on appelle état intriqué de façon maximale un état de la forme

$$|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} e^{i\,\alpha(i)}\, |i_A \otimes i_B\rangle$$

Résumé Le message principal de cette section que afin de décrire l'état d'un système (quantique) constitué de plusieurs sous-systèmes, comme un état à deux qubits, il est nécessaire d'utiliser un opérateur d'état. En effet celui-ci est approrprié pour décrire le mélange d'état formé à partir de vecteurs appartenant aux espaces de Hilbert des sous-systèmes.

3 Théorème de non clonage quantique

Introduction La condition indispensable pour que la méthode de cryptographie quantique décrite précédemment soit parfaitement sûre est que l'espionne *Eve* ne puisse pas reproduire (cloner) l'état de la particule envoyée par Bob à Alice tout en conservant pour elle le résultat de sa mesure, ce qui rendrait l'interception du message indétectable. Que cela ne soit pas possible est garanti par le théorème de non clonage quantique.

Copie d'un état quantique Pour montrer ce théorème, supposons que l'on souhaite dupliquer un état quantique inconnu $|\chi_1\rangle$. Le système sur lequel on veut imprimer la copie est noté $|\varphi\rangle$: c'est

l'équivalent de la feuille blanche. Par exemple, si l'on veut cloner un état de spin 1/2 $|\chi_1\rangle$, $|\varphi\rangle$ est aussi un état de spin 1/2. L'évolution du vecteur d'état dans le processus de clonage doit être de la forme

$$|\chi_1 \otimes \varphi\rangle \longrightarrow |\chi_1 \otimes \chi_1\rangle$$

Cette évolution est régie par un opérateur unitaire U qu'il n'est pas nécessaire de préciser

$$|U(\chi_1 \otimes \varphi)\rangle = |\chi_1 \otimes \chi_1\rangle$$

U doit être universel (car l'opération de photocopie ne peut pas dépendre de l'état à photocopier) et donc indépendant de $|\chi_1\rangle$), qui est inconnu par hypothèse. Bien sûr si $|\chi_1\rangle$ était connu, il n'y aurait pas de problème car la procédure de préparation serait connue. Si l'on veut cloner un second original $|\chi_2\rangle$, on doit avoir

$$|U(\chi_2 \otimes \varphi)\rangle = |\chi_2 \otimes \chi_2\rangle$$

Évaluons maintenant le produit scalaire

$$X = \langle \chi_1 \otimes \varphi | U^\dagger U (\chi_2 \otimes \varphi)\rangle$$

de deux façons différentes

$$\begin{aligned} (1) \quad & X = \langle \chi_1 \otimes \varphi | \chi_2 \otimes \varphi\rangle = \langle \chi_1 | \chi_2 \rangle \\ (2) \quad & X = \langle \chi_1 \otimes \phi_1 | \chi_2 \otimes \chi_2\rangle = (\langle \chi_1 | \chi_2 \rangle)^2 \end{aligned} \tag{3.1}$$

Il en résulte que soit $|\chi_1\rangle \equiv |\chi_2\rangle$, soit $\langle \chi_1 | \chi_2 \rangle = 0$. On peut cloner un état $|\chi_1\rangle$ ou un état orthogonal, mais pas une superposition linéaire des deux.

Analyse Cette preuve du théorème de non clonage explique pourquoi on ne peut pas se restreindre, en cryptographie quantique, à une base d'états de polarisation orthogonaux $\{|x\rangle, |y\rangle\}$ pour les photons. C'est l'utilisation de superpositions linéaires des états de polarisation $|x\rangle$ et $|y\rangle$ qui permet de détecter la présence éventuelle d'un espion. Le théorème de non clonage interdit à *Eve* de cloner le photon envoyé par *Alice* à *Bob* dont la polarisation lui est inconnue ; si elle était capable d'effectuer ce clonage, elle pourrait alors reproduire le photon à un grand nombre d'exemplaires et elle mesurerait sans problème sa polarisation.

> ***Résumé*** Dans cette section on a vu que le principe de superposition est à la base de l'impossibilité de copier un état quantique. En effet en fabriquant la copie de deux états distincts puis en les projetant l'un sur l'autre (en effectuant un produit scalaire) on se rend compte que soit l'un ou l'autre des états est reproduit. Ceci interdit toute combination linéaire qui serait nécessaire pour rendre l'interception d'un message indétectable.

4 La téléportation

La téléportation est une application amusante des états intriqués, qui pourrait avoir des applications pour le transfert de l'information quantique (**Figure 1**). Supposons qu'*Alice* souhaite transférer à *Bob* l'information sur l'état de spin $|\varphi_A\rangle$ d'une particule A de spin 1/2

$$|\varphi_A\rangle = \lambda\,|0_A\rangle + \mu\,|1_A\rangle$$

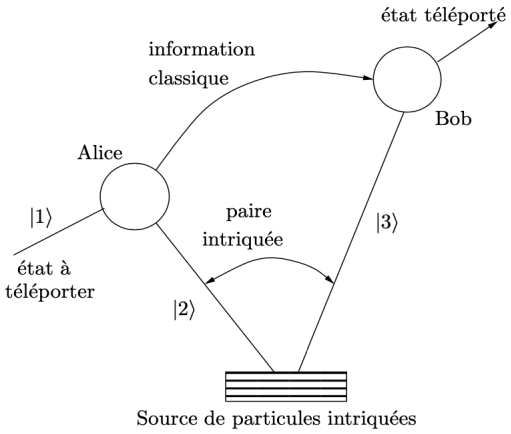

Figure 1: *Téléportation* : *Alice* effectue une *mesure de Bell* sur les qubits A et B, et informe *Bob* du résultat par une voie classique.

qui lui est a priori inconnu, sans lui transmettre directement cette particule.

Elle ne peut pas faire une mesure du spin, car elle ne connaît pas l'orientation du spin de la particule A, et toute mesure projetterait en général $|\varphi_A\rangle$ sur un autre état. Le principe du transfert de l'information consiste à utiliser une paire auxiliaire de particules intriquées B et C de spin $1/2$ partagées par *Alice* et *Bob* : la particule B est utilisée par *Alice* et la particule C est envoyée vers *Bob* (**Figure 1**). Ces particules B et C se trouvent par exemple dans l'état intriqué de spin

$$|\Psi_{BC}\rangle = \frac{1}{\sqrt{2}}\left(|0_B 0_C\rangle + |1_B 1_C\rangle\right)$$

L'état initial des trois particules $|\Phi_{ABC}\rangle$ est donc

$$\begin{aligned} |\Phi_{ABC}\rangle &= \left(\lambda\,|0_A\rangle + \mu\,|1_A\rangle\right) \otimes \left[\frac{1}{\sqrt{2}}\left(|0_B 0_C\rangle + |1_B 1_C\rangle\right)\right] \\ &= \frac{\lambda}{\sqrt{2}}\,|0_A\rangle\left(|0_B 0_C\rangle + |1_B 1_C\rangle\right) + \frac{\mu}{\sqrt{2}}\,|1_A\rangle\left(|0_B 0_C\rangle + |1_B 1_C\rangle\right) \end{aligned} \tag{4.1}$$

où l'on abuse (un peu) de la notation en ne notant plus systématiquement le produit tensoriel $\otimes$. Anticipons un peu en introduisant les portes `cNOT` et de Hadamard `H`. La *porte de Hadamard* agit sur les qubits individuels de la façon suivante

$$\mathtt{H}\,|0_A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \qquad \text{et} \qquad \mathtt{H}\,|1_A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

tandis que la porte `cNOT` est une porte à deux qubits dont l'action est la suivante : elle ne modifie pas le second qubit, ou *qubit cible*, si le premier qubit, ou *qubit de contrôle*, est dans l'état $|0\rangle$, et elle effectue sur le qubit cible l'échange $|0\rangle \leftrightarrow |1\rangle$ si le qubit de contrôle est dans l'état $|1\rangle$. *Alice* va d'abord appliquer sur les qubits A et B une porte `cNOT`, le qubit A jouant le rôle du qubit de contrôle et le qubit B celui de qubit cible (**Figure 2**). Cette opération transforme l'état initial (4.1) des trois qubits en $\mathtt{cNOT}\,|\Phi_{ABC}\rangle = |\Phi'_{ABC}\rangle$ soit

$$|\Phi'_{ABC}\rangle = \frac{\lambda}{\sqrt{2}}\left(|0_A\rangle\,|0_B 0_C\rangle + |0_A\rangle\,|1_B 1_C\rangle\right) + \frac{\mu}{\sqrt{2}}\left(|1_A\rangle\,|1_B 0_C\rangle + |1_A\rangle\,|0_B 1_C\rangle\right) \tag{4.2}$$

Alice applique ensuite une porte de Hadamard sur le qubit A, ce qui transforme (4.2) en $\mathtt{H}\,|\Phi'_{ABC}\rangle = |\Phi''_{ABC}\rangle$ soit

$$\begin{aligned}|\Phi''_{ABC}\rangle \;=\; \frac{1}{2}\,\big[\,&\lambda\,|0_A0_B0_C\rangle + \lambda\,|0_A1_B1_C\rangle + \lambda\,|1_A0_B0_C\rangle + \lambda\,|1_A1_B1_C\rangle\\ &+\mu\,|0_A1_B0_C\rangle + \mu\,|0_A0_B1_C\rangle - \mu\,|1_A1_B0_C\rangle - \mu\,|1_A0_B1_C\rangle\,\big]\end{aligned} \tag{4.3}$$

Cette expression peut de se récrire

$$\begin{aligned}|\Phi''_{ABC}\rangle \;=\; &\frac{1}{2}\,|0_A0_B\rangle\,\big(\,\lambda\,|0_C\rangle + \mu\,|1_C\rangle\,\big)\\ &+\frac{1}{2}\,|0_A1_B\rangle\,\big(\,\mu\,|0_C\rangle + \lambda\,|1_C\rangle\,\big)\\ &+\frac{1}{2}\,|1_A0_B\rangle\,\big(\,\lambda\,|0_C\rangle - \mu\,|1_C\rangle\,\big)\\ &+\frac{1}{2}\,|1_A1_B\rangle\,\big(\,-\mu\,|0_C\rangle + \lambda\,|1_C\rangle\,\big)\end{aligned} \tag{4.4}$$

La dernière opération d'*Alice* consiste à mesurer les deux qubits dans la base $\{|0\rangle, |1\rangle\}$. La mesure conjointe par *Alice* des qubits A et B est appelée *mesure de Bell*. Cette mesure projette la paire (AB) sur l'un des quatre états $|i_Aj_B\rangle$, $i, j = 0, 1$, et le vecteur d'état du qubit C se lit sur chacune des lignes de (4.4).

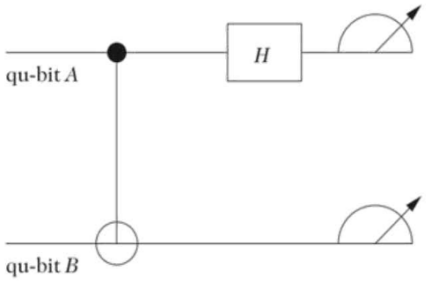

Figure 2: Alice applique une porte `cNOT` sur les qubits A et B puis une *porte de Hadamard* $\mathtt{H}$ sur le qubit A.

Le cas le plus simple est celui où le résultat de la mesure est $|0_A0_B\rangle$. Le qubit C arrive alors à Bob dans l'état

$$\lambda\,|0_C\rangle + \mu\,|1_C\rangle$$

c'est-à-dire dans l'état initial du qubit A, avec les mêmes coefficients λ et μ. *Alice* informe *Bob* par une voie classique (téléphone...) que le qubit va lui arriver dans le même état que le qubit A. Si au contraire elle mesure $|0_A1_B\rangle$, le qubit C est dans l'état

$$\mu\,|0_C\rangle + \lambda\,|1_C\rangle$$

et elle informe *Bob* qu'il doit appliquer au qubit C une rotation de π autour de Ox, ou de façon équivalente la matrice σ_x

$$\exp\left(-i\,\frac{\pi\,\sigma_x}{2}\right) = -i\,\sigma_x$$

Dans le troisième cas $|1_A0_B\rangle$, il faut appliquer une rotation de π autour de Oz, et dans le dernier cas ($|1_A1_B\rangle$) une rotation de π autour de Oy. On note que dans les quatre cas de figure, *Alice* ne

connaît pas les coefficients λ et μ, et elle communique uniquement à *Bob* les informations sur la rotation qu'il doit effectuer. Il est utile d'ajouter les remarques finales :

- à aucun moment les coefficients λ et μ ne sont mesurés, et l'état $|\varphi_A\rangle$ est détruit au cours de la mesure faite par *Alice*. Il n'y a donc pas de contradiction avec le théorème de non clonage ;
- *Bob* ne « connaît » l'état de la particule C que lorsqu'il a reçu le résultat de la mesure d'*Alice*. La transmission de cette information doit se faire par une voie classique, à une vitesse au plus égale à celle de la lumière. Il n'y a donc pas transmission instantanée de l'information à distance ;
- il n'y a jamais transport de matière dans la téléportation.

Résumé Dans cette section on a vu qu'il était possible de transmettre des informations sur un état quantique particulier sans pour autant le mesurer directement. À cette occasion on a utilisé les portes logiques `cNOT` et de Hadamard `H` afin de modifier l'état à plusieurs qutbits que l'on cherche à reproduire sans mesure et sans transmission instantanée d'information.

A Exemple de réalisation physique d'un état intriqué

Il n'est pas évident de construire un état intriqué à partir d'un produit tensoriel. Il est nécessaire d'introduire une interaction entre les deux qubits. Prenons l'exemple de deux spins 1/2. Une interaction possible[4] entre ces deux spins est

$$H = \frac{\hbar\omega}{2}\,\vec{\sigma}_A \cdot \vec{\sigma}_B$$

Utilisons le résultat de l'exercice (B.1)

$$\frac{1}{2}\left(\mathcal{I} + \vec{\sigma}_A \cdot \vec{\sigma}_B\right) |\, i\, j\,\rangle = |\, j\, i\,\rangle$$

pour montrer que

$$\begin{aligned}
(\vec{\sigma}_A \cdot \vec{\sigma}_B)\ \frac{1}{\sqrt{2}}\left(\,|10\rangle + |01\rangle\,\right) &= (\vec{\sigma}_A \cdot \vec{\sigma}_B)\ |\Phi_+\rangle = |\Phi_+\rangle \\
(\vec{\sigma}_A \cdot \vec{\sigma}_B)\ \frac{1}{\sqrt{2}}\left(\,|10\rangle - |01\rangle\,\right) &= (\vec{\sigma}_A \cdot \vec{\sigma}_B)\ |\Phi_-\rangle = -3\,|\Phi_+\rangle
\end{aligned}$$

Les vecteurs $|\Phi_+\rangle$ et $|\Phi_-\rangle$ sont vecteurs propres de $\vec{\sigma}_A \cdot \vec{\sigma}_B$ avec les valeurs propres respectives $+1$ et -3. Partons au temps $t = 0$ d'un état non intriqué, par exemple $|\Phi(t=0)\rangle = |10\rangle$. Pour obtenir son évolution temporelle, il suffit de décomposer cet état sur $|\Phi_+\rangle$ et $|\Phi_-\rangle$ selon

$$|\Phi(t=0)\rangle = \frac{1}{\sqrt{2}}\left(\,|\Phi_+\rangle + |\Phi_-\rangle\,\right)$$

Écrire l'évolution temporelle est alors immédiat

$$\begin{aligned}
e^{iHt}|\Phi(0)\rangle \;&=\; \frac{1}{\sqrt{2}}\left(\,e^{-i\omega t/2}\,|\Phi_+\rangle + e^{3i\omega t/2}\,|\Phi_-\rangle\,\right) \\
&=\; \frac{1}{\sqrt{2}}\,e^{i\omega t/2}\left(\,e^{-i\omega t}\,|\Phi_+\rangle + e^{i\omega t/2}\,|\Phi_-\rangle\,\right) \\
&=\; e^{i\omega t/2}\left(\,\cos(\omega t)\,|10\rangle - i\,\sin(\omega t)\,|01\rangle\,\right)
\end{aligned}$$

Il suffit de choisir $\omega t = \pi/4$ pour obtenir l'état intriqué

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(\,|10\rangle + i\,|01\rangle\,\right)$$

La difficulté vient de ce que H est en général une interaction interne au système, qui, contrairement aux interactions de type externe utilisées pour les qubits individuels, ne peut pas être branchée et débranchée facilement pour ajuster t. Si l'interaction est à courte distance, il est possible de rapprocher puis d'éloigner les deux qubits afin de les faire interagir pendant un temps contrôlé.

[4] Une origine possible de cette interaction pourrait être l'interaction entre les deux moments magnétiques associés aux spins, mais en général il s'agira plutôt d'une interaction d'échange, dont l'origine est le principe d'exclusion de Pauli.

B Exercices

B.1 Indépendance du produit tensoriel par rapport à la base

Supposons que l'on ait construit le produit tensoriel de deux espaces $\mathcal{H}_A$ et $\mathcal{H}_B$ à partir de bases $\{|m_A\rangle\}$ et $\{|n_A\rangle\}$

$$|\varphi_A \otimes \chi_B\rangle = \sum_{m,n} c_m d_n \, |m_A \otimes n_A\rangle$$

Soit $|i_A\rangle$ et $|j_A\rangle$ deux autres bases orthonormées de $\mathcal{H}_A$ et $\mathcal{H}_B$ déduites des bases $\{|m_A\rangle\}$ et $\{|n_A\rangle\}$ par des transformations unitaires respectives R ($R^{-1} = R^*$) et S ($S^{-1} = S^*$)

$$|i_A\rangle = \sum_m R_{in}|m_A\rangle \qquad \text{et} \qquad |j_b\rangle = \sum_n S_{jm}|n_B\rangle$$

Calculer le produit tensoriel $|i \otimes j)\rangle$. Par ailleurs, on peut écrire la décomposition de $|\varphi\rangle$ et $|\chi\rangle$ dans les bases respectives $|i\rangle$ et $|j\rangle$

$$|\varphi\rangle = \sum_{i=1}^{N} \hat{c}_i|i_A\rangle \qquad \text{et} \qquad |\chi\rangle = \sum_{j=1}^{N} \hat{d}_j|j_A\rangle$$

Montrer que

$$\sum_{i,j} \hat{c}_i \, \hat{d}_j \, |i_A \otimes j_A\rangle = |\varphi \otimes \chi\rangle$$

B.2 Propriétés de l'opérateur d'état

1. Montrer à partir de

$$\rho = \sum_i \mathsf{p_i} \, |\mathsf{i}\rangle\langle\mathsf{i}| \qquad\qquad \sum_{\mathsf{i}} \mathsf{p_i} = 1$$

que l'opérateur d'état ρ le plus général doit avoir les propriétés suivantes :

   (a) Il doit être hermitien : $\rho = \rho^*$

   (b) Il doit être de trace unité : $\mathrm{Tr}\,\rho = 1$

   (c) Il doit être positif : $\langle\varphi|\rho|\varphi \geq 0 \quad \forall|\varphi\rangle$

Montrer que la valeur moyenne d'une propriété physique $\mathcal{M}$ est

$$\langle\mathcal{M}\rangle = \mathrm{Tr}(\rho\mathcal{M})$$

2. Montrer de plus que si $\rho^2 = \rho$, alors tous les $\mathsf{p_i}$ sont nuls sauf un seul qui égal à un, et en déduire que la condition $\rho^2 = \rho$ est la condition nécessaire et suffisante pour un état pur.