3.1 Trace partielle et purification

Définition 3.1. *Soit deux espaces d'états A et B. Le trace partielle* $\mathrm{tr_B}$ *est définie par*

$$\mathrm{tr_B}(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2|\mathrm{tr}(|b_1\rangle\langle b_2|)$$

où a_1 et a_2 sont deux vecteurs de l'espace A et b_1 et b_2 sont deux vecteurs de l'espace B

La trace partielle $\mathrm{tr_B}$ d'un état correspond à la matrice densité du premier qubit restant après avoir mesuré le second qubit et oublié cette mesure. Cette interprétation est justifiée par l'égalité mathématique $\mathrm{tr}\left(\mathbf{M}\mathrm{tr_B}(|\psi\rangle)\right) = \mathrm{tr}\left(\mathbf{M} \otimes \mathbf{1}|\psi\rangle\right)$ pour toute observable $\mathbf{M}$.

Lemme 3.2. *Pour $|a\rangle$ et $|b\rangle$ séparés,* $\mathrm{tr_B}(|a\rangle|b\rangle) = |a\rangle\langle a|$. *Pour* $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $\mathrm{tr_B}(|\beta_{00}\rangle\langle\beta_{00}|) = \frac{1}{2}\mathbf{1}$.

Preuve:

$$\begin{aligned}
\mathrm{tr_B}(|\beta_{00}\rangle\langle\beta_{00}|) &= \frac{\mathrm{tr}_2(|00\rangle\langle 00|) + \mathrm{tr}_2(|11\rangle\langle 00|) + \mathrm{tr}_2(|00\rangle\langle 11|) + \mathrm{tr}_2(|11\rangle\langle 11|)}{2} \\
&= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \\
&= \frac{1}{2}\mathbf{1}
\end{aligned}$$

□

Définition 3.3. *Soit ρ une matrice densité sur n qubit et $|\psi\rangle$ un état pur de $n+m$ qubit. Soit S l'espace des m derniers qubit. On dit que l'état pur $|\psi\rangle$ purifie l'état mélangé ρ lorsque* $\mathrm{Tr}_S(|\psi\rangle\langle\psi|) = \rho$.

Théorème 3.4. *Si $2^m \geq \mathrm{rang}(\rho)$, alors il existe une purification de ρ.*

Preuve: Ecrivons la décomposition orthonormale de $\rho = \sum_i \rho_i |i^A\rangle\langle i^A|$. Définissons l'état pur $|\psi\rangle = \sum_i \rho_i |i^A\rangle|i^R\rangle$ qui correspond à ρ combiné avec le système $R = \sum_i p_i |i^R\rangle$.$|\psi\rangle$ est une purification de ρ. En effet :

$$\begin{aligned}
\mathrm{tr}_R(|\psi\rangle\langle\psi|) &= \sum_i \sqrt{p_i p_j}|i^A\rangle\langle j^A|\mathrm{tr}_R(|i^R\rangle\langle j^R|) \\
&= \sum_i p_i |i^A\rangle\langle i^A| \\
&= \rho
\end{aligned}$$

□

3.2 Différences entre la communication quantique et classique

3.2.1 Paradoxe EPR

Alice et Bob reçoivent respectivement les bits aléatoire x et y. Alice et Bob retournent respectivement les bits a et b. Leur objectif est de maximiser $p = Pr_{x,y}(a \oplus b = x \wedge y)$

Cas classique

Une très simple stratégie consiste à jouer $a = b = 0$. Alice et Bob perdent seulement lorsque $x = y = 1$. Cette stratégie réussit donc avec une probabilité $p = \frac{3}{4}$.

xy	ab	$x \wedge y$	$a \oplus b$
00	00	0	0
01	00	0	0
10	00	0	0
11	00	1	0

On ne peut pas faire mieux, même avec une stratégie probabiliste.

Théorème 3.5. *Dans le cas classique, pour toute stratégie probabiliste,* $p \leq \frac{3}{4}$

Preuve: Un protocole probabiliste correspond à une certaine distribution de probabilité sur les protocoles déterministes. Il nous suffit donc de prouver le résultat pour les stratégies déterministes.

Lemme 3.6. *Soit quatre observables* $\mathbf{a}$, $\mathbf{a}'$, $\mathbf{b}$, $\mathbf{b}'$ *à valeur dans* $\{\pm 1\}$. *S'il s'agit de fonctions de variables aléatoires cachées, on peut écrire l'inégalité CHSH*

$$|\langle \mathbf{ab} \rangle + \langle \mathbf{a'b} \rangle + \langle \mathbf{ab'} \rangle - \langle \mathbf{a'b'} \rangle| \leq 2$$

Preuve: On a ou bien $\mathbf{a} + \mathbf{a}' = 0$ et $\mathbf{a} - \mathbf{a}' = \pm 2$, ou bien $\mathbf{a} - \mathbf{a}' = 0$ et $\mathbf{a} + \mathbf{a}' = \pm 2$. On peut donc écrire dans tous les cas :

$$\mathbf{C} = (\mathbf{a} + \mathbf{a}')\mathbf{b} + (\mathbf{a} - \mathbf{a}')\mathbf{b}' = \pm 2$$

Cette égalité découle de l'hypothèse d'une variable cachée. En mécanique quantique, elle correspond à l'idée que des valeurs sont simultanément prises par toutes les variables même s'il s'avère impossible physiquement de mesurer à la fois $\mathbf{a}$ et $\mathbf{a}'$ ou $\mathbf{b}$ et $\mathbf{b}'$. Par inégalité triangulaire :

$$|\langle \mathbf{C} \rangle| \leq |\mathbf{C}| = 2$$

On obtient donc

$$|\langle \mathbf{ab} \rangle + \langle \mathbf{a'b} \rangle + \langle \mathbf{ab'} \rangle - \langle \mathbf{a'b'} \rangle| \leq 2$$

□

Cette inégalité est violée pour certain systèmes quantiques, ce qui permet de réfuter les théories de la mécanique quantique à variables cachées locales. Nous l'utilisons uniquement ici pour majorer la probabilité de succès dans le cas classique.

Soit a_0, a_1 la valeur choisie par Alice pour $x = 0, 1$ et b_0, b_1 la valeur choisie par Bob pour $y = 0, 1$ Définissons les quantités suivantes :

$$\mathbf{a} = (-1)^{a_0} \quad \mathbf{a}' = (-1)^{a_1}$$
$$\mathbf{b} = (-1)^{b_0} \quad \mathbf{b}' = (-1)^{b_1}$$

Posons p_{xy} la probabilité que l'équation soit vérifiée lorsque les bits d'entrée sont x et y

$$\langle \mathbf{ab} \rangle = 2p_{00} - 1 \quad \langle \mathbf{ab}' \rangle = 2p_{01} - 1$$
$$\langle \mathbf{a}'\mathbf{b} \rangle = 2p_{10} - 1 \quad \langle \mathbf{a}'\mathbf{b}' \rangle = 1 - 2p_{11}$$

L'inégalité CHSH s'écrit alors

$$2(p_{00} + p_{01} + p_{10} + p_{11}) - 4 \leq 2$$

$$\langle p \rangle = \frac{1}{4}(p_{00} + p_{01} + p_{10} + p_{11}) \leq \frac{3}{4}$$

□

Cas quantique

Alice et Bob partagent maintenant un état $|\beta_{00}\rangle$ défini par

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Définissons le protocole suivant :

Protocole suivi par ALICE
- **if** $x = 1$ **then**
  - Alice effectue $\mathbf{R}(\frac{3\pi}{16}) \otimes \mathbf{1}$
- **else**
  - Alice effectue $\mathbf{R}(\frac{-\pi}{16}) \otimes \mathbf{1}$
- **end if**
- Alice renvoie le résultat de sa mesure a

Protocole suivi par Bob
- **if** $y = 1$ **then**
  - Bob effectue $\mathbf{1} \otimes \mathbf{R}(\frac{3\pi}{16})$
- **else**
  - Bob effectue $\mathbf{1} \otimes \mathbf{R}(-\frac{\pi}{16})$
- **end if**
- Bob renvoie le résultat de sa mesure b

$R(\theta)$ est la rotation d'angle θ. Cette transformation s'écrit dans la base de mesure

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Théorème 3.7. *Pour ce protocole,* $Pr_{x,y}(a \oplus b = x \wedge y) = \cos^2(\frac{\pi}{8})$.

Preuve: Cet protocole revient à appliquer $\mathbf{R}\left(\frac{(4x-1)\pi}{16}\right)\otimes\mathbf{R}\left(\frac{(4y-1)\pi}{16}\right)$ à $|\beta_{00}\rangle$. On a la formule suivante

$$\mathbf{R}(\theta_1)\otimes\mathbf{R}(\theta_2)=\frac{1}{\sqrt{2}}(\cos(\theta_1+\theta_2)(|00\rangle-|11\rangle)+\sin(\theta_1+\theta_2)(|01\rangle+|10\rangle))$$

On calcule la probabilité que $a\oplus b=x\wedge y$ au cas par cas.
- $x=1$ et $y=1$, on obtient $a\oplus b=1$ avec probabilité $\sin^2(\frac{3\pi}{8})$
- $x=1$ et $y=0$, on obtient $a\oplus b=0$ avec probabilité $\cos^2(\frac{\pi}{8})$
- $x=0$ et $y=1$, on obtient $a\oplus b=0$ avec probabilité $\cos^2(\frac{\pi}{8})$
- $x=0$ et $y=0$, on obtient $a\oplus b=0$ avec probabilité $\cos^2(\frac{\pi}{8})$

On trouve donc $Pr_{x,y}(a\oplus b=x\wedge y)=\cos^2(\frac{\pi}{8})$. □

Le protocole obtenu viole l'inégalité du cas classique car $\cos^2(\frac{\pi}{8})\approx 0{,}853$.

3.2.2 Paradoxe GHZ

Alice, Bob, et Charlie reçoivent respectivement x, y, z avec la condition $x\oplus y\oplus z=0$, c'est-à-dire $xyz\in\{000,011,101,110\}$. Le but est d'obtenir le plus de fois l'égalité $a\oplus b\oplus c=x\vee y\vee z$.

Cas classique

La stratégie $a=x, b=1-y, c=1$ réussit avec une probabilité $p=\frac{3}{4}$.

xyz	abc	$x\vee y\vee z$	$a\oplus b\oplus c$
000	011	0	0
011	001	1	1
101	111	1	1
110	101	1	0

On ne peut pas faire mieux, même avec une stratégie probabiliste.

Théorème 3.8. *Pour toute stratégie probabiliste, la probabilité de succès est inférieure à* $\frac{3}{4}$.

Preuve: Un protocole probabiliste correspond à une certaine distribution de probabilité sur les protocoles déterministes. Il nous suffit donc de prouver le résultat pour les stratégies déterministes.

Notons a_0,a_1 la stratégie d'Alice, b_0, b_1 la stratégie de Bob, et c_0,c_1 la stratégie de Charlie.

$$\begin{cases} a_0\oplus b_0\oplus c_0=0\\ a_0\oplus b_1\oplus c_1=1\\ a_1\oplus b_0\oplus c_1=1\\ a_1\oplus b_1\oplus c_0=1 \end{cases}$$

L'expression constituée par le ou exclusif de tous les éléments de la partie de gauche a pour valeur 0. La même opération appliquée aux éléments de droite donne 1. Il doit donc y avoir au moins une expression qui ne satisfait pas l'égalité, ce qui montre qu'une stratégie déterministe a une probabilité de succès d'au plus $\frac{3}{4}$. □

Cas quantique

Alice, Bob et Charlie partagent maintenant l'état quantique défini par

$$|Q\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

Cet état est appelé état de Greenberger-Horne-Zeilinger (GHZ).

Protocole pour Alice
if $x = 1$ **then**
Appliquer $\mathbf{H} \otimes \mathbf{1} \otimes \mathbf{1}$
end if
Renvoyer la mesure a

Protocole pour Bob
if $y = 1$ **then**
Appliquer $\mathbf{1} \otimes \mathbf{H} \otimes \mathbf{1}$
end if
Renvoyer la mesure b

Protocole pour Charlie
if z=1 **then**
Appliquer $\mathbf{1} \otimes \mathbf{1} \otimes \mathbf{H}$
end if
Renvoyer la mesure c

Théorème 3.9. *Avec ce protocole, $a \oplus b \oplus c$ vaut $x \vee y \vee z$ dans tous les cas.*

Preuve: Cet protocole consiste à appliquer $\mathbf{H}^x \otimes \mathbf{H}^y \otimes \mathbf{H}^z$ à $|Q\rangle$. Démontrons que l'égalité est réalisée pour tout triplet xyz.

- $xyz = 000$, $|Q\rangle$ est mesuré dans l'état initial.
- $xyz = 011$, Le transformation effectuée est

$$\mathbf{1}_A \otimes \mathbf{H}_B \otimes \mathbf{H}_C|Q\rangle = \frac{1}{2}(|001\rangle - |010\rangle - |100\rangle - |111\rangle)$$

- $xyz = 101$

$$\mathbf{H}_A \otimes \mathbf{1}_B \otimes \mathbf{H}_C|Q\rangle = \frac{1}{2}(|001\rangle - |010\rangle - |100\rangle - |111\rangle)$$

- $xyz = 110$

$$\mathbf{H}_A \otimes \mathbf{H}_B \otimes \mathbf{1}_C|Q\rangle = \frac{1}{2}(|001\rangle - |010\rangle - |100\rangle - |111\rangle)$$

Dans tous les cas, $a \oplus b \oplus c = x \vee y \vee z$. □

3.2.3 Superdense Coding

Alice veut faire passer à Bob un message constitué des deux bits x et y à l'aide d'un seul qubit. Alice et Bob partagent la paire $|\beta_{00}\rangle$. Définissons les paires suivantes, appelées états de Bell :

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\beta_{01}\rangle = \tfrac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\beta_{11}\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

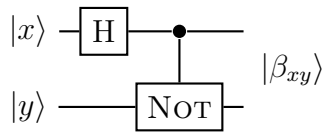

Figure 3.1: Circuit quantique permettant de transformer $|xy\rangle$ en $|\beta_{xy}\rangle$

Lemme 3.10. *On peut passer d'un état de Bell à un autre en appliquant une porte quantique au premier des qubits.*

Preuve:

$$\begin{array}{ll} \mathbf{1}\otimes\mathbf{1}|\beta_{00\rangle} = |\beta_{00}\rangle & \mathbf{NOT}\otimes\mathbf{1}|\beta_{00}\rangle = |\beta_{01}\rangle \\ \mathbf{Z}\otimes\mathbf{1}|\beta_{00}\rangle = |\beta_{10}\rangle & (\mathbf{Z}\circ\mathbf{NOT})\otimes\mathbf{1}|\beta_{00}\rangle = |\beta_{11}\rangle \end{array}$$

□

Le lemme 3.10 signifie qu'Alice peut transformer $|\beta_{00}\rangle$ en n'importe lequel des quatre états de Bell en fonction des bits x et y. Définissons alors le protocole suivant :

if $x = 1$ **then**
  Alice applique $\mathbf{Z}\otimes\mathbf{1}$
end if
if $y = 1$ **then**
  Alice applique $\mathbf{NOT}\otimes\mathbf{1}$
end if
Alice envoie son qubit à Bob

Théorème 3.11. *Ce protocole permet à Alice de communiquer à Bob les deux bits x et y à l'aide d'un seul qubit.*

Preuve: L'état obtenu au terme de cet algorithme est $|\beta_{xy}\rangle$. Bob, au terme de ce protocole, utilise l'inverse du circuit quantique 3.1 pour produire $|xy\rangle$ à partir de $|\beta_{xy}\rangle$ et obtenir ainsi les deux bits initiaux x et y.

□

Dans le cas où une tierce personne intercepte le qubit envoyé par Alice, aucune information n'est obtenue sur x et y car $\mathrm{tr}_{\mathrm{B}}(|\beta_{xy}\rangle) = \frac{1}{2}\mathbf{1}$.

3.2.4 Téléportation quantique

Alice veut transmettre à Bob un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Bob est éloigné et sa position est inconnue. Ils partagent déjà l'état $|00\rangle$. Appelons $|\psi_0\rangle$ l'état initial du système :

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle\otimes|0\rangle\otimes|0\rangle \\ &= \alpha|000\rangle + \beta|100\rangle \end{aligned}$$

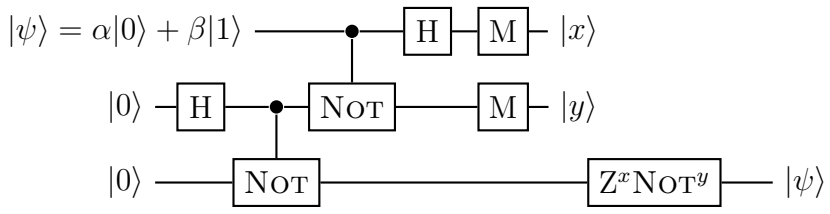

Figure 3.2: Téléportation quantique de l'état $|\psi\rangle$

Théorème 3.12. *Alice peut téléporter l'état $|\psi\rangle$ à Bob.*

Preuve: Le protocole de la téléportation est représenté sur le circuit 3.2. Alice applique une porte d'Hadamard au deuxième qubit.

$$\begin{aligned}
|\psi_1\rangle &= \mathbf{1}\otimes\mathbf{H}\otimes\mathbf{1}|\psi_0\rangle \\
&= \alpha(\mathbf{1}\otimes\mathbf{H}\otimes\mathbf{1})|000\rangle + \beta(\mathbf{1}\otimes\mathbf{H}\otimes\mathbf{1})|100\rangle \\
&= \alpha|0\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle + \beta|0\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle+|010\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle+|110\rangle)
\end{aligned}$$

Alice applique une porte $\mathbf{C-Not}$ du deuxième au troisième qubit.

$$\begin{aligned}
|\psi_2\rangle &= \mathbf{1}\otimes\mathbf{C-Not}|\psi_1\rangle \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle+|011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle+|111\rangle)
\end{aligned}$$

Alice applique une porte $\mathbf{C-Not}$ du premier au deuxième qubit.

$$\begin{aligned}
|\psi_3\rangle &= \mathbf{C-Not}\otimes\mathbf{1}|\psi_2\rangle \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle+|011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle+|101\rangle)
\end{aligned}$$

Alice applique une porte d'Hadamard au premier qubit.

$$\begin{aligned}
|\psi_4\rangle &= \mathbf{H}\otimes\mathbf{1}\otimes\mathbf{1}|\psi_3\rangle \\
&= \frac{\alpha}{\sqrt{2}}\mathbf{H}|0\rangle\otimes(|00\rangle+|11\rangle) + \frac{\beta}{\sqrt{2}}\mathbf{H}|1\rangle(|10\rangle+|01\rangle) \\
&= \frac{\alpha}{2}(|000\rangle+|011\rangle+|100\rangle+|111\rangle) + \frac{\beta}{2}(|010\rangle+|001\rangle-|110\rangle-|101\rangle) \\
&= \frac{1}{2}|00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle) + \frac{1}{2}|01\rangle\otimes(\alpha|1\rangle+\beta|0\rangle) + \frac{1}{2}|10\rangle\otimes(\alpha|0\rangle-\beta|1\rangle) + \frac{1}{2}|11\rangle\otimes(\alpha|1\rangle-\beta|0\rangle)
\end{aligned}$$

Les deux premier qubit sont dans l'un des quatre états suivant $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ et l'état du troisième qubit est respectivement $\alpha|0\rangle+\beta|1\rangle$, $\alpha|1\rangle+\beta|0\rangle$, $\alpha|0\rangle-\beta|1\rangle$, $\alpha|1\rangle-\beta|0\rangle$. Alice

mesure maintenant les deux premiers qubit de l'état $|\psi_4\rangle$, réduisant cet état à l'un des quatre termes de la somme précédente.

$$|\psi_5\rangle = \begin{cases} |00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) & \text{avec probabilité } 1/4 \\ |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) & \text{avec probabilité } 1/4 \\ |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) & \text{avec probabilité } 1/4 \\ |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle) & \text{avec probabilité } 1/4 \end{cases}$$

Notons x et y l'état des deux premiers qubits obtenus par Alice au terme de la mesure. Bob, après avoir pris connaissance de x et y, n'a plus qu'à effectuer une simple opération sur le troisième qubit pour retrouver $|\psi\rangle$:

$$|\psi_6\rangle = \mathbf{1} \otimes \mathbf{1} \otimes \mathbf{Z}^x\mathbf{NOT}^y|\psi_5\rangle$$

En conclusion, le qubit $|\psi\rangle$ a bien été téléporté à Bob. □

On peut montrer que la trace partielle du système $|\psi_4\rangle$ par rapport à l'espace du système d'Alice est $\frac{1}{2}\mathbf{1}$, c'est-à-dire qu'elle ne dépend pas de $|\psi\rangle$. Avant de recevoir la mesure d'Alice, Bob n'a donc aucune information sur $|\psi\rangle$. La téléportation respecte donc les autres théories physiques en ne permettant pas de transmettre de l'information plus vite que la lumière.

Réalisations expérimentales :

- 1 photons [Zeilinger et al : Innsbruck'97]
- 1 photon, 6 km [Gisin et al : Genève'02]
- 1 atome [Blatt et al : Innsbruck'04]