TD 1 : Algèbre linéaire, qubits et portes quantiques

UE Informatique quantique et Recherche opérationnelle
Module 1 : Informatique quantique

29 novembre 2022

ENSIIE, C. Grange

Exercice 1 (Système composite et produit tensoriel)**.**

Pour décrire un système quantique à plusieurs états dans un espace de Hilbert, on utilise le produit tensoriel. Par exemple, un système composite à deux états vit dans un espace $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, où A et B sont nommés les sous-systèmes du système AB.

1. *Calculer les produits tensoriels suivants :* $\begin{pmatrix}1\\2\end{pmatrix} \otimes \begin{pmatrix}3\\4\end{pmatrix}$ *et* $\begin{pmatrix}0\\1\\7\end{pmatrix} \otimes \begin{pmatrix}4\\0\\2\end{pmatrix}$.

2. *Soient deux états quantiques* $|\psi_A\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle)$ *et* $|\psi_B\rangle = \frac{-i}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$. *Écrire l'état* $|\psi_A\rangle \otimes |\psi_B\rangle$. *De quelle norme est-il ? Conclure, et généraliser pour deux états* $|\psi_A\rangle = \alpha_A|0\rangle + \beta_A|1\rangle$ *et* $|\psi_B\rangle = \alpha_B|0\rangle + \beta_B|1\rangle$.

3. *Quelle est la dimension de l'espace de Hilbert utilisé pour décrire un état à deux qubits ? En donner une base.*

4. *Soit* $|\phi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{2}{\sqrt{3}}|1\rangle$. *Exprimer les états* $|+\rangle|0\rangle$, $|\phi\rangle|-\rangle$ *et* $|\phi\rangle|\phi\rangle$ *dans la base de la question précédente.*

5. *Quelle est la dimension de l'espace de Hilbert utilisé pour décrire un espace à 3 qubits ? A 2 qutrits ? Généraliser au cas n-qudits, et en donner une base.*

Correction : Dimensions : 2^3, 3^2 et cas général d^n.

Exercice 2 (Mesure et projection)**.**

La mesure d'un état quantique $|\psi\rangle$ *est la projection le long d'un axe ou dans un sous-espace. Pour cela, on définit au préalable* l'appareil de mesure *comme un ensemble de projecteurs* $\{P_n\}$ *tels que* $\sum_n P_n = I$, *où* $\{n\}$ *est l'ensemble des résultats observables. Ainsi, le résultat de la mesure de* $|\psi\rangle$ *dans cette base de mesure est* $|\phi_n\rangle = \frac{P_n|\psi\rangle}{\|P_n|\psi\rangle\|}$ *avec probabilité* $\langle\psi|P_n|\psi\rangle$.

1. *Quels sont les projecteurs qui correspondent à la mesure dans la base* $\{|0\rangle, |1\rangle\}$ *? Quels sont les résultats possibles de la mesure de* $|0\rangle$ *dans cette base ? Avec quelles probabilités ? Justifier.*

2. *Montrer que le circuit Figure 1 effectue une mesure dans la base* $\{|+\rangle, |-\rangle\}$. *Tester avec le vecteur* $|+\rangle$, *resp.* $|-\rangle$, *pour vérifier que ce vecteur donne bien 0, resp. 1, avec une probabilité 1. Tester ensuite avec les qubits* $|0\rangle$ *et* $|1\rangle$. *Enfin, quels sont les projecteurs* P_+ *et* P_- *utilisés ?*

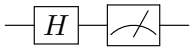


Figure 1: Circuit de mesure dans $\{|0\rangle, |1\rangle\}$.

3. *Soit la base tournée de l'angle* θ *décrite par* $\{\cos(\theta)|0\rangle + \sin(\theta)|1\rangle, -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle\}$. *Vérifier que c'est une base, la visualiser, puis répondre aux mêmes questions de précédemment pour cette base.*

Correction : projecteur sur l'état $|i\rangle$ vaut $|i\rangle\langle i|$. Projecteurs :

- $|0\rangle\langle 0|$ et $|1\rangle\langle 1|$
- $|+\rangle\langle +|$ et $|-\rangle\langle -|$
- Bien visualiser la nouvelle base. Projecteurs : $\begin{pmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{pmatrix}$ et $\begin{pmatrix} \sin^2\theta & -\cos\theta\sin\theta \\ -\cos\theta\sin\theta & \cos^2\theta \end{pmatrix}$

Exercice 3 (Opérations sur des états à 1 qubit)**.** *Soit* U *une porte unitaire à 1 qubit. Nous allons voir qu'il est possible de décomposer une telle porte de façon générique. Nous rappelons la définition des portes de rotations autour des axes* Y *et* Z *de la sphère de Bloch. Soit* $\theta \in \mathbb{R}$,

$$R_Y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$

$$R_Z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}.$$

1. *Nous allons montrer que* U *peut être décomposée* par rapport à Y et Z, *i.e. comme une composition de rotation autour de ces axes. Justifier qu'il existe des réels* α, β, γ *et* δ *tels que*

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

.

Nous allons montrer qu'il est possible de produire n'importe quel état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ *à partir de l'état* $|0\rangle$ *de façon générique. Soit la matrice de phase* $\mathrm{Ph}(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$, *pour* $\phi \in \mathbb{R}$.

2. *Pour* θ *et* ϕ *des réels, calculer l'état final* $|\psi\rangle$ *du circuit Figure 2, puis conclure.*

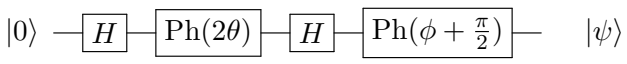


Figure 2: Décomposition avec porte de phase.

3. *Trouver le couple* (θ, ϕ) *pour produire l'état* $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, *puis pour l'état* $|\psi\rangle = i|1\rangle$. *Trouvez-vous un autre moyen de produire ces états ?*

Correction :
Question 1 : Puisque U est unitaire, ses colonnes et lignes sont orthonormales, d'où l'existence de ces réels.

$$U = \begin{pmatrix} e^{i(\alpha-\frac{\beta}{2}-\frac{\delta}{2})}\cos\frac{\gamma}{2} & -e^{i(\alpha-\frac{\beta}{2}+\frac{\delta}{2})}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\frac{\beta}{2}-\frac{\delta}{2})}\sin\frac{\gamma}{2} & e^{i(\alpha+\frac{\beta}{2}+\frac{\delta}{2})}\sin\frac{\gamma}{2} \end{pmatrix}.$$

Question 2 : $\mathrm{Ph}(\phi+\frac{\pi}{2})H\mathrm{Ph}(2\theta)H\left|0\right\rangle = e^{i\theta}\begin{pmatrix}\cos\theta \\ e^{i\phi}\sin\theta\end{pmatrix}$, ainsi, modulo une phase globale, on a en sortie l'état $\cos\theta\left|0\right\rangle + e^{i\phi}\sin\theta\left|1\right\rangle$.
Pour $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$, on résout le système

$$\begin{cases}\alpha = \cos\theta \\ \beta = e^{i\phi}\sin\theta\end{cases}$$

avec $\theta \in [0,\pi[$ et $\phi \in [0,2\pi[$. On a un unique couple de solution. Remarque : si α est un complexe, on l'écrit sous forme polaire $\alpha = re^{i\phi_\alpha}$ et on considère $e^{i\phi_\alpha}$ dans la phase globale, ce qui nous ramène au cas $\alpha \in \mathbb{R}$.
Pour $\left|\psi\right\rangle = \frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}} = H\left|0\right\rangle$: $(\theta,\phi) = (\frac{\pi}{4},\pi)$,
Pour $\left|\psi\right\rangle = i\left|1\right\rangle = Y\left|0\right\rangle$: $(\theta,\phi) = (\frac{\pi}{2},\frac{\pi}{2})$.

Exercice 4 (Codage superdense)**.**

Dans cet exercice, nous examinons le codage superdense qui consiste à communiquer deux bits d'information en n'envoyant qu'un seul qubit. Cela illustre l'avantage que peut donner l'informatique quantique sur les communications.
Supposons qu'Alice et Bob peuvent communiquer via un canal quantique et qu'ils partagent ensemble l'état $\left|\beta_{00}\right\rangle = \frac{\left|00\right\rangle+\left|11\right\rangle}{\sqrt{2}}$*. Alice veut envoyer deux bits d'information à Bob (00, 10, 01 ou 11). Elle procède ainsi :*

- *Si elle désire envoyer 00, elle ne fait rien*
- *Si elle désire envoyer 10, elle applique la porte X à son qubit*
- *Si elle désire envoyer 01, elle applique la porte Z à son qubit*
- *Si elle désire envoyer 11, elle applique la porte iY à son qubit*

1. *Pour chaque cas, écrire le nouvel état quantique obtenu après l'opération effectuée par Alice.*
2. *Après avoir effectué son opération, Alice envoie son qubit à Bob. Montrer que Bob peut retrouver les deux bits d'information qu'Alice voulait lui transmettre.*

Bob détient alors une paire qui est un des 4 états de Bell. Comme c'est une base, il peut les discriminer et en déduire les 2 bits d'information d'Alice.

Exercice 5 (Interférences destructives)**.**

Dans cet exercice, nous allons illustrer la différence qui peut exister entre les algorithmes probabilistes classiques et les algorithmes quantiques. Nous illustrons ici la différence entre un état quantique et une information manquante (ou variable cachée).

1. *Quelle est la probabilité de mesurer 0, respectivement 1, en sortie du circuit qui applique deux fois la porte de Hadarmard H à $\left|0\right\rangle$?*

2. *Considérons l'algorithme suivant :*

   - *Application de H à $|0\rangle$, puis on mesure :*
   - *Si le résultat vaut 0, on créé un nouveau circuit en appliquant H de nouveau à $|0\rangle$,*
   - *Sinon, on créé un nouveau circuit en appliquant H à $|1\rangle$.*

   Quelle est la probabilité de mesurer 0, resp. 1, en sortie de l'algorithme ?

3. *Ces deux approches semblent identiques d'un point de vue probabiliste. Expliquer pourquoi les résultats diffèrent néanmoins.*

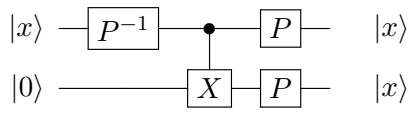
Correction : C'est l'amplitude du "dernier" 1 qui est égale à l'opposé du "premier" 1 qui font qu'elles s'annulent pour le premier circuit. Cela illustre la différence entre un état quantique et une information manquante/une variable cachée. Le qubit n'est pas un 0 ou un 1 qui aurait été fixé en début de circuit et dont on ne connaît la vraie valeur qu'à la fin du circuit, car alors c'est le comportement du second circuit qu'on observerait. Il s'agit d'un vrai mélange entre $|0\rangle$ et $|1\rangle$ jusqu'à ce que l'on mesure.

Exercice 6 (Non-clonage)**.** *Soient les qubits $|e_1\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$ et $|e_2\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$.*

1. *Montrer que $\{|e_1\rangle, |e_2\rangle\}$ est une base orthonormale.*

2. *Trouver une porte A qui clone uniquement les qubits de cette base, i.e.*
$$A|x\rangle|0\rangle \mapsto |x\rangle|x\rangle ,$$
   si et seulement si $x = e_1$ ou $x = e_2$. Démontrer qu'aucun autre qubit n'est cloné par A. Indice : Trouver A pour la base $\{|0\rangle, |1\rangle\}$ puis faire un changement de base.

Correction : Pour la base $\{|0\rangle, |1\rangle\}$, A est la porte CNOT. De plus, la matrice changement de base de $\{|0\rangle, |1\rangle\}$ vers $\{|e_1\rangle, |e_2\rangle\}$ est $P = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$; $P^{-1} = \frac{1}{-i\sqrt{2}}\begin{pmatrix} -i & -1 \\ -i & 1 \end{pmatrix}$. Ainsi,



avec $x = e_1$ ou $x = e_2$.

Exercice 7 (Paradoxe EPR)**.** *Nous allons examiner un jeu où la meilleure stratégie quantique bat la meilleure stratégie classique.*

Règles du jeu et objectif :

- *Alice et Bob partagent une information en amont, mais ne peuvent communiquer ensemble pendant la durée du jeu.*
- *Alice, resp. Bob, reçoit un bit aléatoire x, resp. y.*
- *Alice, resp. Bob, renvoit un bit a, resp. b.*
- *Objectif : maximiser le gain $g = \mathbb{P}_{x,y}(a \oplus b = x \wedge y)$.*

Déroulement classique du jeu :

1. *Écrire les tables de vérités de $a \oplus b$ et $x \wedge y$. En déduire la meilleure stratégie déterministe pour Alice et Bob, ainsi que la valeur du gain g associée.*

On admet par la suite que la meilleur stratégie probabiliste n'est pas meilleure que la meilleure stratégie déterministe.
Déroulement quantique du jeu : on suppose maintenant que Alice et Bob partagent une paire EPR $\beta_{00} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Le protocole est le suivant :

- *Bob effectue une rotation d'angle θ (à déterminer)*
- *Si $x = 1$, Alice effectue une rotation d'angle 2θ*
- *Si $y = 1$, Bob effectue une rotation d'angle -2θ*

2. *Ecrire l'état quantique obtenu pour chaque couple de valeurs différentes (x, y).*
3. *En déduire la valeur du gain g en fonction de θ. Pour quelle valeur de θ le gain est-il maximum ?*

Correction : Cas déterministe : $g = \frac{3}{4}$; cas quantique : pour $\theta = \frac{\pi}{8}$, on a $g = \cos^2(\frac{\pi}{8}) \simeq 0.85$.