ENSEIRB-MATMECA
Option second semestre, 2014/2015

Information Quantique

Examen- 20 Mai 2015

Durée : 2H
Documents autorisés : tous documents autorisés.
Indications : les trois exercices sont indépendants.
Notation : le barème est indicatif.
La note finale est min(20, note-ex1+note-ex2+note-ex3).

Exercice 1 (/4 pts)

Théorème de non-clonage.

Il s'agit de prouver une version du théorème de non-clonage plus forte que celle vue en cours.
Soit $\mathcal{B}$ un espace de Hilbert de dimension 2. On note $(|0\rangle, |1\rangle)$ une base orthonormée de $\mathcal{B}$, $|b\rangle$ un vecteur unitaire de $\mathcal{B}$, $\mathcal{H}$ un espace de Hilbert de dimension finie $n \geq 0$ et $|c\rangle$ un vecteur unitaire de $\mathcal{H}$.
On veut montrer qu'il n'existe pas de transformation unitaire

$$U : \mathcal{B} \otimes \mathcal{B} \otimes \mathcal{H} \to \mathcal{B} \otimes \mathcal{B} \otimes \mathcal{H}$$

qui permette de *cloner* les états de $\mathcal{B}$ au sens suivant : $\forall |\Phi\rangle \in \mathcal{B}, \exists |d\rangle \in \mathcal{H}$

$$U |\Phi\rangle \otimes |b\rangle \otimes |c\rangle = |\Phi\rangle \otimes |\Phi\rangle \otimes |d\rangle \tag{1}$$

Supposons qu'une transformation unitaire U vérifiant (1) existe.
Considérons des états $|\Phi\rangle, |\Psi\rangle \in \mathcal{B}$ et $|d\rangle, |d'\rangle \in \mathcal{H}$ tels que (1) est vraie ainsi que son analogue ((2) :

$$U |\Psi\rangle \otimes |b\rangle \otimes |c\rangle = |\Psi\rangle \otimes |\Psi\rangle \otimes \left|d'\right\rangle \tag{2}$$

1- Montrer que

$$\langle\Phi|\Psi\rangle \left(\langle\Phi|\Psi\rangle \left\langle d|d'\right\rangle - 1\right) = 0$$

2- En déduire que $|\Phi\rangle, |\Psi\rangle$ sont orthogonaux ou colinéaires.
Indication : on pourra utiliser le cas d'égalité dans l'inégalité de Cauchy-Schwarz.
3- Combien de droites vectorielles de $\mathcal{B}$ un système quantique peut-il "cloner" ?

Exercice 2 (/10 pts)

Théorème de non-effacement.

On veut prouver un énoncé qui est plus ou moins "inverse" de celui de l'exercice 1.

Informellement : un système quantique ne peut, à partir de tout "clone"

$$|\Phi\rangle \otimes |\Phi\rangle \otimes |d\rangle$$

engendrer un état $|\Phi\rangle \otimes |N\rangle \otimes |c\rangle$ tel que le vecteur $|N\rangle$ est fixe (N évoque l'idée de "neutre") et $|N\rangle \otimes |c\rangle$ a "perdu la mémoire" de $|\Phi\rangle$. Autrement dit : il n'est pas possible d'*effacer* la copie de $|\Phi\rangle$.

Dans ce qui suit la notation pour les produits tensoriels de vecteurs $|u\rangle \otimes |v\rangle \ldots$ sera souvent abrégée en $|u\rangle |v\rangle \ldots$. La notation $\mathcal{B}$ désigne un espace de Hilbert de dimension 2 et on fixe une base orthonormée $(|0\rangle, |1\rangle)$ de $\mathcal{B}$.

1- Montrer qu'il n'existe pas de transformation unitaire

$$U : \mathcal{B} \otimes \mathcal{B} \to \mathcal{B} \otimes \mathcal{B}$$

et de vecteurs $|N\rangle \in \mathcal{B}$ tels que, pour tout $|\Phi\rangle \in \mathcal{B}$,

$$U |\Phi\rangle |\Phi\rangle = |\Phi\rangle |N\rangle .$$

2- Donner un exemple de transformation unitaire $U : \mathcal{B}\otimes\mathcal{B}\otimes\mathcal{B} \to \mathcal{B}\otimes\mathcal{B}\otimes\mathcal{B}$ et de vecteurs unitaires [1] $|N\rangle, |A\rangle \in \mathcal{B}$ tels que, pour tous $|\Phi\rangle \in \mathcal{B}$, il existe $|A'\rangle \in \mathcal{B}$

$$U |\Phi\rangle |\Phi\rangle |A\rangle = |\Phi\rangle |N\rangle \left|A'\right\rangle .$$

Aide : penser à la porte SWAP.

Formellement : voici le théorème de non-effacement.

Théorème :soit $\mathcal{H}$ un espace de Hilbert de dimension finie ; soit une transformation unitaire $U : \mathcal{B} \otimes \mathcal{B} \otimes \mathcal{H} \to \mathcal{B} \otimes \mathcal{B} \otimes \mathcal{H}$ et des vecteurs unitaires $|N\rangle \in \mathcal{B}, |A\rangle \in \mathcal{H}$ tels que, pour tout $|\Phi\rangle \in \mathcal{B}$, il existe $|A'\rangle \in \mathcal{H}$:

$$U |\Phi\rangle |\Phi\rangle |A\rangle = |\Phi\rangle |N\rangle \left|A'\right\rangle \tag{3}$$

alors il existe une transformation unitaire $D : \mathcal{B} \otimes \mathcal{H} \to \mathcal{B} \otimes \mathcal{H}$ telle que, pour tout $|\Phi\rangle \in \mathcal{B}$

$$(\mathrm{Id}_{\mathcal{B}} \otimes D) \circ U |\Phi\rangle |\Phi\rangle |A\rangle = |\Phi\rangle |\Phi\rangle |A\rangle \tag{4}$$

1. l'épithète " unitaire" a été précisé au tableau le jour de l'examen

(La lettre D évoque un *décodage* de l'état $|\Phi\rangle$ qui a été caché par U). Le but des questions qui suivent est de *démontrer* ce théorème.

On suppose que $U, |N\rangle, |A\rangle$ vérifient la propriété (3). Notons $|A_0\rangle, |A_1\rangle$ les vecteurs de $\mathcal{H}$ tels que

$$U|0\rangle|0\rangle|A\rangle = |0\rangle|N\rangle|A_0\rangle \text{ et } U|1\rangle|1\rangle|A\rangle = |1\rangle|N\rangle|A_1\rangle.$$

Soit $|\Phi\rangle \in \mathcal{B}$. Il est donc de la forme $\alpha|0\rangle + \beta|1\rangle$ pour des coefficients $\alpha, \beta \in \mathbb{C}$. Notons $|A(\alpha,\beta)\rangle$ le vecteur de $\mathcal{H}$ tel que

$$U|\Phi\rangle|\Phi\rangle|A\rangle = |\Phi\rangle|N\rangle|A(\alpha,\beta)\rangle. \tag{5}$$

3- Montrer qu'il existe un vecteur unitaire fixe $|F\rangle \in \mathcal{B}\otimes\mathcal{B}\otimes\mathcal{H}$ tel que, pour tous $\alpha, \beta \in \mathbb{C}$:

$$\alpha^2|0\rangle|N\rangle|A_0\rangle + \beta^2|1\rangle|N\rangle|A_1\rangle + \sqrt{2}\alpha\beta|F\rangle = \alpha|0\rangle|N\rangle|A(\alpha,\beta)\rangle + \beta|1\rangle|N\rangle|A(\alpha,\beta)\rangle \tag{6}$$

4- Montrer que l'application : $\mathbb{C}^2 \to \mathcal{H}$ définie par $(\alpha,\beta) \mapsto |A(\alpha,\beta)\rangle$ est linéaire.
5- En déduire que , pour tout $(\alpha,\beta) \in \mathbb{C}^2$, $|A(\alpha,\beta)\rangle = \alpha|A_0\rangle + \beta|A_1\rangle$.
6- Montrer que $|F\rangle = \frac{1}{\sqrt{2}}[|0\rangle|N\rangle|A_1\rangle + |1\rangle|N\rangle|A_0\rangle]$.
7- Montrer que $(|A_0\rangle, |A_1\rangle)$ est une famille orthonormée.
8- Exhiber une transformation unitaire D qui ait la propriété (4).
9- Sous les hypothèses du théorème, est-il toujours vrai qu'il existe une transformation unitaire $\mathrm{D} : \mathcal{B}\otimes\mathcal{H} \to \mathcal{B}\otimes\mathcal{H}$ telle que,

$$(\mathrm{Id}_{\mathcal{B}} \otimes D) \circ U = \mathrm{Id}_{\mathcal{B}\otimes\mathcal{B}\otimes\mathcal{H}}?$$

Exercice 3(/10 pts)
Cryptographie quantique.

On étudie le procole de [Bennett 1992]. Ce protocole repose sur un codage à deux états seulement à la différence du protocole [BB84] qui reposait sur un codage à quatre états.
On réutilise les notations de [BB84] : $|\uparrow\rangle, |\nearrow\rangle, |\rightarrow\rangle, |\searrow\rangle$ pour désigner certains vecteurs et $\oplus, \otimes$ pour désigner certaines bases.
Alice tire aléatoirement un bit x et le transmet par :

$$\begin{aligned} |\uparrow\rangle \quad &\text{si} \quad x = 0 \\ |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle) \quad &\text{si} \quad x = 1 \end{aligned}$$

Bob tire aléatoirement un bit y et en déduit une base B_B de la façon suivante :

$$\begin{aligned} B_B := \oplus \quad &\text{si} \quad y = 0 \\ B_B := \otimes \quad &\text{si} \quad y = 1 \end{aligned}$$

De plus Bob associe au *résultat* de la mesure μ_B (du qbit de A, dans la base B_B) un bit b de la façon suivante

$$\begin{aligned} b := 0 \quad &\text{si} \quad \mu_B = |\uparrow\rangle \text{ ou } \mu_B = |\nearrow\rangle \\ b := 1 \quad &\text{si} \quad \mu_B = |\rightarrow\rangle \text{ ou } \mu_B = |\searrow\rangle . \end{aligned}$$

1- Montrer que le résultat $b = 1$ ne peut être obtenu que si les bits x et y sont différents.

Notation : pour décrire un envoi de N qbits par A, on notera $x_0, x_1, \ldots, x_i, \ldots, x_{N-1}$ les bits d'Alice, $y_0, y_1, \ldots, y_i, \ldots, y_{N-1}$ les bits de Bob et $b_0, b_1, \ldots, b_i, \ldots, b_{N-1}$ les bits obtenus par Bob en appliquant le protocole de communication.

2- Comment Alice et Bob peuvent-ils constituer une clé secrète connue d'eux seuls ?
3- Si n est le nombre de bits transmis quel est (en moyenne) le nombre de bits de la clé ?

On étudie maintenant une attaque de Eve. Eve connait le protocole de communication de A et B [2]. Elle adopte la stratégie suivante : elle tire aléatoirement une base B_E ($\oplus$ ou $\otimes$) et effectue une mesure μ_E du qbit de A dans cette base ;

— si $B_E = \oplus$ et $\mu_E = |\uparrow\rangle$, alors elle renvoie $|\uparrow\rangle$ à Bob
— si $B_E = \otimes$ et $\mu_E = |\nearrow\rangle$, alors elle renvoie $|\nearrow\rangle$ à Bob
— si $B_E = \oplus$ et $\mu_E = |\rightarrow\rangle$, alors elle renvoie $|\nearrow\rangle$ à Bob
— si $B_E = \otimes$ et $\mu_E = |\searrow\rangle$, alors elle renvoie $|\uparrow\rangle$ à Bob

4- Supposons que $x = 0$, $B_E = \otimes$, $\mu_E = |\nearrow\rangle$, Eve applique sa stratégie, $y = 0$ et B obtient $\mu_B = |\rightarrow\rangle$.
4.1 Vérifier que $b = 1$.
4.2 Est-il vrai que $x \neq y$? Cette remarque contredit-elle votre réponse à la question 1 ?
4.3 Cette interception par E peut-elle être détectée par A et B ?
4.4 Eve connaît-elle le bit x de A ?
5- Supposons que $x = 0$, $B_E = \otimes$, $\mu_E = |\searrow\rangle$, Eve applique sa stratégie et $y = 0$.
5.1 Vérifier que $b = 0$.
5.2 Cette interception par E peut-elle être détectée par A et B ?
5.3 Eve connaît-elle le bit x de A ?
6- 6.1 Définir un protocole de vérification pour A et B leur permettant de détecter Eve aussi souvent que possible (on pourra s'inspirer du protocole de Bennett et Brassard 84 vu en cours).
6.2 Quelle probabilité E a-t-elle d'être détectée lorsqu'elle intercepte n qbits qui sont tous vérifiés par A,B ?
Aide : on pourra envisager tous les cas de figure pour les données $(x, B_E, \mu_E, y, \mu_B)$.
6.3 Supposons que A et B ont "sacrifié" m bits pour tester la présence d'Ève et que Ève a effectivement intercepté ces m qbits. Quelle est la probabilité que E soit détectée ?
Attention : A et B ne sacrifient pas des bits *quelconques* (comme en 6.2), mais seulement ceux pour lesquels la détection est possible (voir questions 4,5).

Supposons que E a intercepté n qbits envoyés par A et retenus dans la clé finale. Il s'agit des envois d'indice $i_1 < \ldots < i_j < \ldots < i_n$. On suppose que A et B n'ont pas détecté E (malgré des tests effectués sur *d'autres* qbits que les n qbits dont nous discutons).
8.1 En moyenne combien y-a-t-il de positions de bits dont la valeur est

2. et les lois de la mécanique quantique

différente dans la clé de A et dans la clé de B ?
8.2 Y-a-t-il des bits de la clé de A que E est *certaine* de connaitre ? Combien y-en-a-t-il en moyenne ?
9- E effectue un *pari* X_E sur la valeur du bit x selon la stratégie suivante :

B_E	μ_E	X_E
$\oplus$	$\|\uparrow\rangle$	0
$\oplus$	$\|\rightarrow\rangle$	1
$\otimes$	$\|\nearrow\rangle$	1
$\otimes$	$\|\searrow\rangle$	0

On considère que x, y, B_E sont aléatoires, indépendants, chacun suivant une loi de " pile ou face" (les deux valeurs possibles ont chacune une probabilité $\frac{1}{2}$) et que les mesures μ_E, μ_B suivent les lois de la mécanique quantique.

9.1 Que vaut $\Pr(X_E = x | b = 1)$ (la probabilité que $X_E = x$ sachant que $b = 1$) ? i.e. quelle est la probabilité, avec cette stratégie, que Ève devine correctement le bit d'Alice, sachant que le bit a été inclus dans la clé finale ?
9.2 Ève applique la stratégie ci-dessus à chacune de ses interceptions sur les indices $i_1, \ldots, i_j, \ldots, i_n$: elle obtient une suite de bits $X_{i_1}, \ldots, X_{i_j}, \ldots, X_{i_n}$ et elle forme le mot

$$C_E := X_{i_1} \cdots X_{i_j} \cdots X_{i_n}$$

En moyenne, combien de bits de C_E sont identiques à ceux de la portion de clé $C_A := x_{i_1} \ldots x_{i_j} \ldots x_{i_n}$?