ENSEIRB-MATMECA
Option second semestre, 2012/2013

Information Quantique

DM- Avril 2013

Indications : Version amendée (le 10/04/2013) grâce aux remarques des étudiants.

Partie 1

Transmission d'information.

Dans cette première partie, on se propose de montrer que, encoder n bits avec k qbits n'est possible que si $k \geq n$.
On fixe $k, n \in \mathbb{N}$ avec $k \leq n$. On note $\mathcal{B}$ l'espace de Hilbert canonique, de dimension 2 et l'on note $|0\rangle, |1\rangle$ sa base canonique. On remarque que $\mathcal{B}^{\otimes k}$ est de dimension $d := 2^k$ sur $\mathbb{C}$

Encodage : On encode chaque vecteur booléen $x \in \mathbb{B}^n$ par un vecteur unitaire $|\Phi_x\rangle \in \mathcal{B}^{\otimes k}$.

Décodage : Soit $|\Phi\rangle \in \mathcal{B}^{\otimes k}$ un vecteur unitaire. On le décode comme suit. On fixe une suite de ℓ observables $\mathcal{H}_0, \ldots, \mathcal{H}_i, \ldots, \mathcal{H}_{\ell-1}$ et une suite de 2^n réels positifs $(\lambda_x)_{x \in \mathbb{B}^n}$, distincts. L'opérateur hermitien associé à $\mathcal{H}_i$ a pour matrice M_i, de dimension d. Pour chaque $x \in \mathbb{B}^n$ et $i \in [0, \ell - 1]$, on note $E_{i,x}$ le sous-espace propre de M_i associé à la valeur propre λ_x.
On tire aléatoirement un indice $i \in [0, \ell - 1]$ suivant une loi de probabilité $(q_0, \ldots, q_i, \ldots, q_{\ell-1})$ (où $q_i > 0$ et $\sum_{i=0}^{\ell-1} q_i = 1$). Autrement dit : la probabilité de tirer l'indice i vaut q_i. Puis on mesure la grandeur $\mathcal{H}_i$ sur l'état $|\Phi\rangle$:
- si la mesure fournit λ_x alors le résultat du décodage est x.
- si le résultat de la mesure n'est aucun λ_x ($x \in \mathbb{B}^n$) alors le décodage échoue.

1- à quelle condition sur les observables $\mathcal{H}_0, \ldots, \mathcal{H}_i, \ldots, \mathcal{H}_{\ell-1}$ est-il vrai que, pour tout vecteur unitaire $|\Phi\rangle \in \mathcal{B}^{\otimes k}$, presque sûrement, le décodage de $|\Phi\rangle$ fournit un vecteur booléen $x \in \mathbb{B}^n$?

On essaye de décoder un vecteur unitaire $|\Phi\rangle \in \mathcal{B}^{\otimes k}$. Pour tout $x \in \mathbb{B}^n$, on note $\Pr(\delta = x)$ la probabilité que la procédure de décodage aboutisse à la valeur x. On définit l'opérateur linéaire

$$P_x := \sum_{i=0}^{\ell-1} q_i P_{i,x}$$

où $P_{i,x}$ est la projection orthogonale sur le sous-espace $E_{i,x}$.

2- Montrer que $\Pr(\delta = x) = \langle\Phi| P_x |\Phi\rangle$
3- Montrer que $\langle\Phi| P_x |\Phi\rangle \leq \mathrm{tr}(P_x)$
4- Vérifier que, dans les conditions de la question 1,

$$\sum_{x\in\mathbb{B}^n} P_x = \mathrm{Id}_d$$

On note p_x la probabilité que la procédure de décodage, appliquée à $|\Phi_x\rangle$ fournisse x.

5- Vérifier que $p_x = \langle\Phi_x| P_x |\Phi_x\rangle$
6- Montrer que $\sum_{x\in\mathbb{B}^n} p_x \leq d$
7- En déduire que, si $k < n$, il existe une vecteur booléen $x \in \mathbb{B}^n$ qui est "mal décodé" en ce sens que : $p_x \leq 2^{k-n}$.
8- Le résultat de la question 7 contredit-il la possibilité du "codage super-dense" vu en cours ?

Partie 2

Complexité de communication
le problème du couplage caché.

Alice et Bob souhaitent résoudre un problème algorithmique. A possède une donnée x_A et B possède une donnée x_B. A peut envoyer des qbits à B mais B ne peut rien envoyer à A. Ils cherchent à fournir la réponse à une question portant sur (x_A, x_B) en *minimisant* le nombre de qbits qu'Alice envoie à Bob.

Donnée de A : $x \in \mathbb{B}^{[0,2N-1]}$
Donnée de B : un couplage $C \subseteq [0, N-1] \times [N, 2N-1]$
Question : fournir un couple $((i,j), x_i \oplus x_j)$ tel que $(i,j) \in C$.

N.B. Un *couplage* sur $[0, 2N-1]$ est le graphe d'une bijection de $[0, N-1]$ dans $[N, 2N-1]$.

Notation : on pose $\lceil log_2(2N) \rceil := n$; il sera ici commode de noter, étant donné un entier $i \in [0, 2N-1]$, $|i\rangle$ le produit tensoriel

$$|i\rangle := |b_n\rangle \otimes |b_{n-1}\rangle \otimes \ldots \otimes |b_i\rangle \ldots \otimes |b_0\rangle \in \mathcal{B}^{\otimes n}$$

tel que

$$i = \sum_{j=0}^{n} b_j 2^j.$$

Un algorithme pour $N = 2$
- Alice calcule le vecteur

$$|\Phi\rangle := \frac{1}{2}[(-1)^{x_0}|0\rangle + (-1)^{x_1}|1\rangle + (-1)^{x_2}|2\rangle + (-1)^{x_3}|3\rangle]$$

- Elle envoie $|\Phi\rangle$ à Bob
- Bob fait une mesure dans la base (orthonormée)

$$(\frac{1}{\sqrt{2}}(|0\rangle + |C(0)\rangle),\ \ \frac{1}{\sqrt{2}}(|0\rangle - |C(0)\rangle),\ \ \frac{1}{\sqrt{2}}(|1\rangle + |C(1)\rangle),\ \ \frac{1}{\sqrt{2}}(|1\rangle - |C(1)\rangle))$$

- Bob renvoie :

$((i, C(i)), 0)$ si sa mesure a projeté $|\Phi\rangle$ sur $\frac{1}{\sqrt{2}}(|i\rangle + |C(i)\rangle)$

$((i, C(i)), 1)$ si sa mesure a projeté $|\Phi\rangle$ sur $\frac{1}{\sqrt{2}}(|i\rangle - |C(i)\rangle)$

1- Montrer que, pour tout $i \in [0, 1]$,la probabilité que Bob obtienne l'état $\frac{1}{\sqrt{2}}(|i\rangle + |C(i)\rangle)$ est

$$\frac{1}{8}((-1)^{x_i} + (-1)^{x_{C(i)}})^2$$

et la probabilité que Bob obtienne l'état $\frac{1}{\sqrt{2}}(|i\rangle - |C(i)\rangle)$ est

$$\frac{1}{8}((-1)^{x_i} - (-1)^{x_{C(i)}})^2$$

2- Montrer que Bob donne presque sûrement une réponse correcte.

Un algorithme pour $2N = 2^n$ En vous inspirant de l'algorithme ci-dessus donner un algorithme dans le cas général.
3- Alice calcule un vecteur $|\Phi\rangle :=?$
- Elle envoie $|\Phi\rangle$ à Bob
4- Bob fait une mesure dans une base orthonormée $\bigcup_{i \in [0, N-1]} \{|u_{i,1}\rangle, |u_{i,-1}\rangle\}$.

- Bob renvoie :
- $((i, C(i)), 0)$ si sa mesure a projeté $|\Phi\rangle$ sur $|u_{i,1}\rangle$
- $((i, C(i)), 1)$ si sa mesure a projeté $|\Phi\rangle$ sur $|u_{i,-1}\rangle$

Quelle base orthonormée lui conseillez-vous de choisir ?

5- Pour tout $i \in [0, N-1]$ et $\varepsilon \in \{1, -1\}$, calculer la probabilité que Bob obtienne l'état $|u_{i,\varepsilon}\rangle$.

6- Bob donne-t-il *presque sûrement* une réponse correcte ?

7- Combien de qbits Alice a-t-elle envoyé à Bob ?