ENSEIRB-MATMECA
Option second semestre, 2012/2013

Information Quantique

Corrigé du DM- Avril 2013

Partie 1

Transmission d'information.

1- Il faut et il suffit que , pour tout $i \in [0, \ell - 1]$, le spectre de M_i soit inclus dans $\{\lambda_x \mid x \in \mathbb{B}^n\}$. Prouvons-le.
1.1 Si $\mathrm{Sp}(M_i) \subseteq \{\lambda_x \mid x \in \mathbb{B}^n\}$, pour tout i, la mesure de $\mathcal{H}_i$ donne un résultat appartenant à $\mathrm{Sp}(M_i)$ (postulat de la mesure) donc le décodage fournit bien un vecteur booléen.
1.2 Supposons que, pour un $i \in [0, \ell - 1]$, un réel $\lambda \notin \{\lambda_x \mid x \in \mathbb{B}^n\}$ est vecteur propre de M_i. Soit $|\Phi\rangle$ un vecteur propre, unitaire, de M_i pour la valeur propre λ :

$$M_i |\Phi\rangle = \lambda |\Phi\rangle$$

Alors, si on tire l'indice i, la mesure de $\mathcal{H}_i$ donnera presque sûrement le résultat λ et le décodage échouera. Donc la probabilité que le décodage échoue dans l'état $|\Phi\rangle$ est $\geq q_i > 0$.
2- Lorsqu'on mesure l'observable $\mathcal{H}_i$ sur un système physique dans l'état $|\Phi\rangle$, la probabilité d'obtenir le résultat λ_x est

$$\Pr(\mu_i = \lambda_x) = \| P_{i,x} |\Phi\rangle \|^2 = \langle \Phi | P_{i,x} |\Phi\rangle . \tag{1}$$

Puisque l'on mesure $\mathcal{H}_i$ avec probabilité q_i , on obtient donc

$$\begin{aligned}
\Pr(\delta = x) = &\quad \textstyle\sum_{i=0}^{\ell-1} q_i \Pr(\mu_i = \lambda_x) \\
= &\quad \textstyle\sum_{i=0}^{\ell-1} q_i \langle \Phi | P_{i,x} |\Phi\rangle \quad \text{(par(1))} \\
= &\quad \langle \Phi | \left(\textstyle\sum_{i=0}^{\ell-1} q_i P_{i,x}\right) |\Phi\rangle \quad \text{(par linéarité)} \\
= &\quad \langle \Phi | P_x |\Phi\rangle \quad \text{(par def. de } P_x\text{)}
\end{aligned}$$

3- Dans une base orthonormée de vecteurs propres de M_i, la matrice de $P_{i,x}$ est de la forme :

$$\begin{pmatrix} \mathrm{I}_m, \mathrm{O}_{m,d-m} \\ \mathrm{O}_{d-m,m}, \mathrm{O}_{d-m,d-m} \end{pmatrix}$$

où m est la dimension de $E_{i,x}$. Donc, si $|\Phi\rangle$ a pour coordonnés dans cette même base :

$$\begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_m \\ \vdots \\ \varphi_d \end{pmatrix}$$

$$\begin{aligned} \langle\Phi| P_{i,x} |\Phi\rangle &= \sum_{j=1}^{m} |\varphi_j|^2 \\ &\leq m \\ &= \mathrm{tr}(P_{i,x}). \end{aligned} \tag{2}$$

(en fait cet argument est valable pour tout opérateur linéaire diagonalisable dans une base orthonormée).
Comme l'application "trace" est linéaire (sur l'espace vectoriel des opérateurs linéaires) on déduit des inégalités (2) pour tous les indices i que

$$\langle\Phi| P_x |\Phi\rangle \leq \mathrm{tr}(P_x).$$

4- La condition de la question 1 est que, pour tout $i \in [0, \ell - 1]$:

$$\mathcal{B}^{\otimes k} = \bigoplus_{x \in \mathbb{B}^n} E_{i,x}$$

Comme $P_{i,x}$ est la projection (orthogonale) sur $E_{i,x}$, on a bien, pour tout vecteur $|\Phi\rangle \in \mathcal{B}^{\otimes k}$ que

$$|\Phi\rangle = \sum_{x \in \mathbb{B}^n} P_{i,x} |\Phi\rangle$$

donc on a bien, pour tout $i \in [0, \ell - 1]$,

$$\mathrm{Id}_d = \sum_{x \in \mathbb{B}^n} P_{i,x} \tag{3}$$

et par combinaison linéaire avec les coefficients q_i de toutes les égalités (3)

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

5- Selon l'égalité établie à la question 3 pour un vecteur unitaire quelconque, $p_x = \langle \Phi_x | P_x | \Phi_x \rangle$.
6-

$$\begin{aligned}
\sum_{x \in \mathbb{B}^n} p_x = & \quad \sum_{x \in \mathbb{B}^n} \langle \Phi_x | P_x | \Phi_x \rangle \quad (\text{ par q.5 }) \\
\leq & \quad \sum_{x \in \mathbb{B}^n} \mathrm{tr}(P_x) \quad (\text{ par q.3 }) \\
= & \quad \mathrm{tr}(\sum_{x \in \mathbb{B}^n} P_x) \quad (\text{ par linéarité de la trace}) \\
= & \quad \mathrm{tr}(\mathrm{Id}_d) \quad (\text{ par q.4}) \\
= & \quad d
\end{aligned}$$

7- Comme $\mathrm{Card}(\mathbb{B}^n) = 2^n$, si, pour tout vecteur booléen $x \in \mathbb{B}^n$: $p_x > \frac{d}{2^n}$, alors

$$\sum_{x \in \mathbb{B}^n} p_x > \sum_{x \in \mathbb{B}^n} \frac{d}{2^n} = d.$$

Cette inégalité contredirait celle de la q.6, ce qui est impossible. Donc il existe un vecteur booléen $x \in \mathbb{B}^n$ tel que $p_x \leq \frac{d}{2^n}$.
8- À première vue, dans le " codage super-dense", Alice réussit à transmettre 2 bits d' information à Bob en ne lui envoyant, physiquement, qu'un seul qbit. Cependant, Alice et Bob ont utilisé un second qbit, intriqué avec le premier ; certes il n'est pas transmis de Alice vers Bob, mais, dans le cadre d'un processus de codage-décodage, il doit être comptabilisé comme une partie du support de l'information.

Partie 2

Complexité de communication
le problème du couplage caché.

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

$$\begin{aligned}
|\frac{1}{\sqrt{2}}(\langle i| + \langle C(i)|) |\Phi\rangle|^2 = & \quad \tfrac{1}{2}|(\langle i|\Phi\rangle + \langle C(i)|\Phi\rangle|^2 \\
= & \quad \tfrac{1}{2}|\tfrac{1}{2}(-1)^{x_i} + \tfrac{1}{2}(-1)^{x_{C(i)}}|^2 \\
= & \quad \tfrac{1}{8}[(-1)^{x_i} + (-1)^{x_{C(i)}}]^2 \quad (\text{module d'un nombre réel}).
\end{aligned}$$

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

$$|\frac{1}{\sqrt{2}}(\langle i| - \langle C(i)|)\,|\Phi\rangle\,|^2 = \quad \tfrac{1}{2}|(\langle i|\Phi\rangle - \langle C(i)|\Phi\rangle\,|^2$$
$$= \quad \tfrac{1}{2}|\tfrac{1}{2}(-1)^{x_i} - \tfrac{1}{2}(-1)^{x_{C(i)}}|^2$$
$$= \quad \tfrac{1}{8}[(-1)^{x_i} - (-1)^{x_{C(i)}}]^2 \quad .$$

2- Pour chaque $i \in [0,1]$, Bob répond $((i,C(i)), x_i \oplus x_{C(i)})$ ssi :
- il répond $((i,C(i)),0)$ et $x_i \oplus x_{C(i)} = 0)$ ou
- il répond $((i,C(i)),1)$ et $x_i \oplus x_{C(i)} = 1)$
ce qui est équivalent à :
- il répond $((i,C(i)),0)$ et $[(-1)^{x_i} + (-1)^{x_{C(i)}})]^2 = 4$ (cas $i,0$) ou
- il répond $((i,C(i)),1)$ et $[(-1)^{x_i} - (-1)^{x_{C(i)}})]^2 = 4$ (cas $i,1$)
D'après la question 1, dans le cas $i,0$,

$$\Pr(\text{Bob répond } ((i,C(i)),0)) = \frac{1}{2}.$$

et dans le cas $i,1$,

$$\Pr(\text{Bob répond } ((i,C(i)),1)) = \frac{1}{2}.$$

Bob donne chacune des deux réponses correctes avec probabilité $\frac{1}{2}$. Il répond donc correctement avec probabilité 1.
3- Essayons le vecteur

$$|\Phi\rangle := \frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} (-1)^{x_i}\,|i\rangle$$

4- Prenons

$$|u_{i,1}\rangle := \frac{1}{\sqrt{2}}(|i\rangle + |C(i)\rangle), \;\; |u_{i,-1}\rangle := \frac{1}{\sqrt{2}}(|i\rangle - |C(i)\rangle).$$

5- Soit $i \in [0, N-1]$. La probabilité que Bob obtienne l'état $|u_{i,\varepsilon}\rangle$ est

$$|\frac{1}{\sqrt{2}}(\langle i| + \varepsilon\,\langle C(i)|)\,|\Phi\rangle\,|^2 = \quad \tfrac{1}{2}\cdot\tfrac{1}{2N}|(\langle i|\Phi\rangle + \varepsilon\,\langle C(i)|\Phi\rangle\,|^2$$
$$= \quad \tfrac{1}{2}|\cdot\tfrac{1}{2N}|(-1)^{x_i} + \varepsilon(-1)^{x_{C(i)}}|^2$$
$$= \quad \tfrac{1}{4N}[(-1)^{x_i} + \varepsilon(-1)^{x_{C(i)}}]^2 \qquad \text{(module d'un nombre réel)}$$

Cette probabilité vaut :

$$\frac{1}{N} \text{ si } (-1)^{x_i} = \varepsilon(-1)^{x_{C(i)}}, \;\; 0 \text{ si } (-1)^{x_i} = -\varepsilon(-1)^{x_{C(i)}}.$$

6- Donc Bob répond, avec probabilité $\frac{1}{N}$, le couple $((i, C(i)), x_i \oplus x_{C(i)})$. Comme ces N réponses sont correctes, Bob donne, avec probabilité 1, une réponse correcte.
7- Alice a envoyé le vecteur $|\Phi\rangle$ qui est écrit sur n qbits, c'est à dire sur seulement $\log_2(N) - 1$ qbits. C'est ce faible nombre de qbits échangés qui est remarquable : avec une information seulement de longueur $\log_2(N)$ sur la donnée de A, B réussit presque sûrement à répondre à une question qui concerne la donnée globale (x, C). Il n'existe pas d'algorithme équivalent, classique déterministe ou classique probabiliste.
Référence :I. Kerenididis, "an introduction to quantum information and applications", `http://www.liafa.univ-paris-diderot.fr/~magniez/epit12/`.