ENSEIRB-MATMECA
Option second semestre, 2011/2012

Information Quantique

Corrigé de l' examen du 21 Mai 2012

Notation : la note finale est
min(20,note-ex1+note-ex2).

Exercice 1 (/20 pts)

Circuits quantiques.

1- On cherche une matrice unitaire R telle que $R^2 = \mathsf{N\hat{O}T}$,
Une méthode possible consiste à réduire $\mathsf{N\hat{O}T}$ à une forme diagonale PDP^{-1} (P est la matrice de passage et D est une matrice diagonale) puis à choisir $R := PD'P^{-1}$ où D' est une racine carrée de D (il y a 4 choix possibles pour D' car chaque valeur propre possède 2 racines carrées dans $\mathbb{C}$). Dans le cas de $\mathsf{N\hat{O}T}$:
les valeurs propres sont $1, -1$ (car, vue comme une application linéaire sur $\mathbb{R}^2$, il s'agit de la symétrie par rapport à la première bissectrice) associées aux vecteurs propres (de norme 1 et orthogonaux) :

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}.$$

Donc

$$P = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}, \;\; P = P^{-1}, \;\; D = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix},$$

On peut choisir, par exemple

$$R := P\begin{pmatrix}1 & 0\\0 & i\end{pmatrix}P^{-1} = \frac{1}{2}\begin{pmatrix}1+i & 1-i\\1-i & 1+i\end{pmatrix}$$

2-

$$\mathsf{T\hat{O}F}\,|x_1, x_2, x_3\rangle = |x_1, x_2, x_3 \oplus x_1x_2\rangle$$

Donc

$$\begin{aligned}\mathsf{T\hat{O}F}\,|x_1, x_2, x_3\rangle = &\quad |x_1, x_2, x_3\rangle &&\text{si } x_1x_2 = 0\\ = &\quad |x_1, x_2\rangle \otimes \mathsf{N\hat{O}T}\,|x_3\rangle &&\text{si } x_1x_2 = 1\end{aligned}$$

ce qui est la définition de $\Lambda^2(\mathsf{N\hat{O}T})$.
3- Le circuit T est un produit de 5 portes. Considérons la valeur du vecteur d'état après chaque porte (on commence par la valeur d'entrée puis on écrit les 5 valeurs successives obtenues) :

$$\begin{array}{ccccccc}
\begin{pmatrix}0\\0\\z\end{pmatrix} & & \begin{pmatrix}0\\0\\z\end{pmatrix} & \begin{pmatrix}0\\0\\z\end{pmatrix} & \begin{pmatrix}0\\0\\z\end{pmatrix} & \begin{pmatrix}0\\0\\z\end{pmatrix} & \begin{pmatrix}0\\0\\z\end{pmatrix} \\
\begin{pmatrix}1\\0\\z\end{pmatrix} & \begin{pmatrix}1\\0\\z\end{pmatrix} & \begin{pmatrix}1\\1\\z\end{pmatrix} & \begin{pmatrix}1\\1\\R^{-1}z\end{pmatrix} & \begin{pmatrix}1\\0\\R^{-1}z\end{pmatrix} & \begin{pmatrix}1\\0\\z\end{pmatrix} \\
\begin{pmatrix}1\\0\\z\end{pmatrix} & & \begin{pmatrix}1\\0\\Rz\end{pmatrix} & \begin{pmatrix}0\\1\\Rz\end{pmatrix} & \begin{pmatrix}0\\1\\z\end{pmatrix} & \begin{pmatrix}0\\1\\z\end{pmatrix} & \begin{pmatrix}0\\1\\z\end{pmatrix} \\
\begin{pmatrix}1\\1\\z\end{pmatrix} & \begin{pmatrix}1\\1\\Rz\end{pmatrix} & \begin{pmatrix}1\\0\\Rz\end{pmatrix} & \begin{pmatrix}1\\0\\Rz\end{pmatrix} & \begin{pmatrix}1\\1\\Rz\end{pmatrix} & \begin{pmatrix}1\\1\\R^2z\end{pmatrix}
\end{array}$$

On voit donc que ce circuit a l' effet suivant les vecteurs de la base canonique :

$$\begin{pmatrix}x_1\\x_2\\z\end{pmatrix} \mapsto \begin{pmatrix}x_1\\x_2\\z\end{pmatrix}$$

si $x_1x_2 = 0$,

$$\begin{pmatrix}x_1\\x_2\\z\end{pmatrix} \mapsto \begin{pmatrix}x_1\\x_2\\R^2z\end{pmatrix}$$

si $x_1x_2 = 1$, Il coïncide donc avec $\Lambda^2(\mathsf{N\hat{O}T})$ sur la base canonique, et par linéarité, il coïncide avec $\Lambda^2(\mathsf{N\hat{O}T})$ sur tout l'espace des états : il calcule l'opérateur de Toffoli.
4- Soit $U : \mathcal{B} \to \mathcal{B}$ une application linéaire unitaire. Alors U est diagonalisable (dans une base orthonormée) :

$$U = PDP^{-1}$$

avec P matrice unitaire. On peut donc appliquer le raisonnement de la question 1 : soit D' une matrice diagonale telle que $D'^2 = D$. Comme les éléments

de la diagonale de D' sont de module 1, la matrice D' est unitaire, et comme P, P^{-1} sont unitaires, la matrice

$$V := PD'P^{-1}$$

est une racine carrée unitaire de U.
5- On peut construire un circuit C_U sur le modèle du circuit T, mais en remplaçant la porte R par la porte V : voir la figure 1.
6- Désignons par $\mathcal{G}_0$ l' ensemble des portes élémentaires $\{\mathsf{cN\hat{O}T}\} \cup \{\Lambda^1(W), W \in$

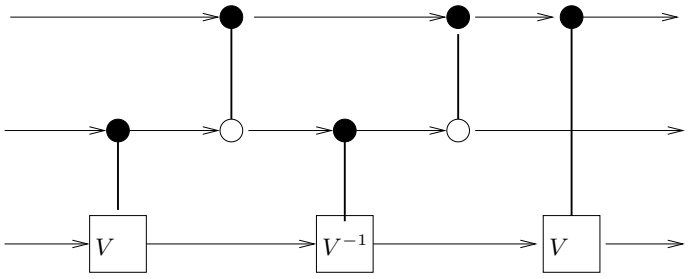

FIGURE 1 – Le circuit C_U

$\mathsf{U}(2)\}$.
Afin de résoudre cette question par récurrence sur k, étendons la définition de $\Lambda^k(U)$ au cas où U est un opérateur unitaire sur $\mathcal{B}^\ell$ (où ℓ est un entier strictement positif) : pour tous $x_1, \ldots, x_k \in \mathcal{B}, y \in \mathcal{B}^{\otimes \ell}$:

$$\begin{aligned} \Lambda^k(U)\,|x_1, \ldots, x_k, y\rangle = &\quad |x_1, \ldots, x_k\rangle \otimes |y\rangle \qquad \text{si } x_1 x_2 \cdots x_k = 0 \\ = &\quad |x_1, \ldots, x_k\rangle \otimes U\,|y\rangle \qquad \text{si } x_1 x_2 \cdots x_k = 1 \end{aligned}$$

Montrons maintenant, par récurrence sur k, la propriété :

$$\forall U \in \mathsf{U}, \Lambda^k(U) \text{ est calculable par un circuit} C_k, \text{ de taille } \leq 5^{k-1} \text{ sur } \mathcal{G}_0.$$

Si $k = 1$, $\Lambda^1(U)$ est une porte de $\mathcal{G}_0$.
Si $k = 2$, $\Lambda^2(U)$ est calculable par le circuit C_U fourni à la question 5, qui n'utilise que des portes de $\mathcal{G}_0$ et qui est de longueur 5.
Soit $k \geq 3$. La matrice U admet une racine carrée unitaire V (question 4) et $V' := \Lambda^{k-2}(V)$ est une racine carrée de $U' := \Lambda^{k-2}(U)$.
On peut appliquer la construction de la question 5, à l'opérateur $\Lambda^2(U')$: le circuit T, dans lequel on remplace R par V', calcule $\Lambda^k(U)$ (notons-le $T[V'/R]$). Par hypothèse de récurrence, $\Lambda^1(V') = \Lambda^{k-1}(V)$ est calculable

par un circuit C_{k-1} de longueur $\leq 5^{k-2}$ sur $\mathcal{G}_0$. En remplaçant, dans le circuit $T[V'/R]$, chaque porte $\Lambda^1(V')$ par le circuit C_{k-1}, on obtient un circuit C_k, de longueur $\leq 5^{k-1}$ sur $\mathcal{G}_0$, qui calcule $\Lambda^k(U)$.
Une analyse plus fine de la longueur de C_k donne :

$$|C_1| = 1, \;\; |C_{k+1}| = 3|C_k| + 2$$

d'où $|C_k| = 2 \cdot 3^{k-1} - 1$.

Exercice 2(/29 pts)
Algorithme de Grover

1- Notons

$$|y_-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \;\; |y_+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

On vérifie que

$$\langle y_s | y_t \rangle = \delta_{s,t} \text{ pour } s, t \in \{+, -\},$$

et on sait que

$$\langle x | x' \rangle = \delta_{x,x'} \text{ pour } x, x' \in \{0, 1\}.$$

Considérons la famille des 2^{n+1} vecteurs :

$$(|x\rangle \, |y_s\rangle)_{x \in \mathbb{B}^n, s \in \{+,-\}} \tag{1}$$

Le produit scalaire de deux d'entre eux vérifie :

$$\langle y_s | \, \langle x | x' \rangle \, | y_t \rangle = \langle x | x' \rangle \, \langle y_s | y_t \rangle = \delta_{x,x'} \delta_{s,t}$$

Donc cette famille est orthonormée.

$$\begin{aligned}
\langle \alpha | \alpha \rangle &= (\frac{1}{\sqrt{N-M}})^2 \sum_{f(x)=0} \langle y_- | \, \langle x | x \rangle \, | y_- \rangle \\
&= (\frac{1}{N-M}) \sum_{f(x)=0} 1 \\
&= (\frac{1}{N-M})(N-M) \\
&= 1.
\end{aligned}$$

Un calcul similaire montre que $\langle \beta | \beta \rangle = 1$.
Les ensembles de vecteurs $\{|x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \mid f(x) = 0\}$ et $\{|x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \mid f(x) = 1\}$

sont des parties disjointes de la famille orthogonale (1). Donc les sous-espaces engendrés par ces ensembles sont orthogonaux. Comme $|\alpha\rangle$ appartient au premier sous-espace et $|\beta\rangle$ au second, $\langle\alpha|\beta\rangle = 0$.
2- Les coefficients

$$c_\alpha := \sqrt{\frac{N-M}{N}}, c_\beta := \sqrt{\frac{M}{N}}$$

satisfont

$$|\psi\rangle = c_\alpha |\alpha\rangle + c_\beta |\beta\rangle$$

3-

$$\cos(\theta') = \frac{c_\alpha}{c_\alpha^2 + c_\beta^2} = \sqrt{\frac{N-M}{N}}, \ \ \sin(\theta') = \frac{c_\beta}{c_\alpha^2 + c_\beta^2} = \sqrt{\frac{M}{N}}.$$

Comme $\cos(\theta') \geq 0$, $\theta' := Arcsin\sqrt{\frac{M}{N}}$ est une mesure de l'angle $(|\alpha\rangle, |\psi\rangle)$.
4- On vérifie que, pour tout $x \in \mathbb{B}^n$,

$$\mathrm{O}\,|x\rangle\,|y_-\rangle = (-1)^{f(x)}\,|x\rangle\,|y_-\rangle$$

Il découle que :

$$\mathrm{O}\,|\alpha\rangle = |\alpha\rangle\,, \ \ \mathrm{O}\,|\beta\rangle = -\,|\beta\rangle\,,$$

et par linéarité :

$$\mathrm{O}\,|\psi\rangle = c_\alpha\,|\alpha\rangle - c_\beta\,|\beta\rangle\,.$$

5- La famille des 2^{n+1} vecteurs :

$$(|x\rangle\,|b\rangle)_{x\in\mathbb{B}^n, b\in\{0,1\}} \tag{2}$$

est aussi une famille orthonormée de $\mathcal{B}^{\otimes(n+1)}$. Comme elle est de cardinal 2^{n+1} qui est la dimension de $\mathcal{B}^{\otimes(n+1)}$. c'est une *base* orthonormée. La définition de S_0 montre que :
- sur le sous-espace P_0 engendré par $|0^n\rangle\,|0\rangle\,, |0^n\rangle\,|1\rangle$, S_0 vaut l' identité,
- sur le sous-espace Q_0 engendré par $|x\rangle\,|0\rangle\,, |x\rangle\,|1\rangle$ (pour $x \in \mathbb{B}^n \setminus \{0^n\}$, S_0 vaut l' opposée de l' identité.
Comme (2) est une base orthonormée, en fait $Q_0 = P_0^\perp$.
Donc S_0 coincide bien avec la symétrie orthogonale par rapport à P_0.
6- Si S est une symétrie par rapport au sous-espace I et parallèlement au sous-espace D alors, pour tout isomorphisme $F : \mathcal{B}^{\otimes(n+1)} \to \mathcal{B}^{\otimes(n+1)}$ l' application $F \circ S \circ F^{-1}$ est la symétrie par rapport au sous-espace FI et parallèlement au sous-espace FD. En prenant $S = S_0$ et $F = H^{\otimes n} \otimes \mathrm{Id}$ on obtient donc que : S_Ψ est la symétrie par rapport au sous-espace $H^{\otimes n} \otimes \mathrm{Id} P_0$ et parallèlement au sous-espace $H^{\otimes n} \otimes \mathrm{Id}(P_0)^\perp$.

La transformation $H^{\otimes n} \otimes \mathrm{Id}$ envoie $|0\rangle$ sur ψ et $|1\rangle$ sur ψ'. L'espace des vecteurs invariants de S_Ψ est donc le plan (complexe) engendré par les vecteurs $|\psi\rangle, |\psi'\rangle$.
Comme la transformation $H^{\otimes n} \otimes \mathrm{Id}$ est unitaire, la direction de la symétrie est aussi $(H^{\otimes n} \otimes \mathrm{Id} P_0)^\perp$, i.e. S_ψ est la symétrie *orthogonale* par rapport au plan (complexe) engendré par les vecteurs $|\psi\rangle, |\psi'\rangle$.
7- On a vu à la question 4 que

$$\mathrm{O}\,|\alpha\rangle = |\alpha\rangle\,, \quad \mathrm{O}\,|\beta\rangle = -\,|\beta\rangle\,, \tag{3}$$

Donc O laisse le plan P globalement invariant.

$$S_\psi\,|\psi\rangle = |\psi\rangle$$

Soit $|\psi''\rangle := \cos(\theta' + \pi/2)\,|\alpha\rangle + \sin(\theta' + \pi/2)\,|\beta\rangle$. Comme l'angle $(|\psi\rangle, |\psi''\rangle)$ a pour mesure $\pi/2$, $|\psi''\rangle \perp |\psi\rangle$. Par ailleurs $|\psi''\rangle \perp |\psi'\rangle$, car $|\psi''\rangle$ appartient au sous-espace vectoriel (complexe) engendré par $\{|x\rangle\,|y_-\rangle \mid x \in \mathbb{B}^n\}$ alors que $|\psi'\rangle$ appartient au sous-espace vectoriel (complexe) engendré par $\{|x\rangle\,|y_+\rangle \mid x \in \mathbb{B}^n\}$. On en conclut que $|\psi''\rangle \in P_0^\perp$, ce qui entraine que

$$S_\psi\,|\psi\rangle = -\,|\psi\rangle\,, \quad S_\psi\,\big|\psi''\big\rangle = -\,\big|\psi''\big\rangle\,. \tag{4}$$

Comme $|\psi\rangle, |\psi''\rangle$ est une base de P (sur $\mathbb{R}$), S_ψ laisse le plan P globalement invariant.
8- Les équations (3) montrent que $\tilde{\mathrm{O}}$ est une symétrie orthogonale par rapport à $|\alpha\rangle$. Les équations (4) montrent que $\tilde{S_\psi}$ est une symétrie orthogonale par rapport à $|\psi\rangle$. Donc $\tilde{S_\psi}\tilde{\mathrm{O}}$ est la rotation de P d'angle double de l'angle entre les axes des symétries i.e. $\theta = 2\theta'$.
9.1- Notons par $(\widehat{|u\rangle, |v\rangle})$ l' angle orienté entre 2 vecteurs et $\mu((\widehat{|u\rangle, |v\rangle})) \in$

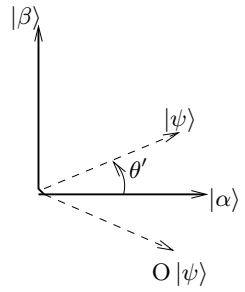

FIGURE 2 – Le plan P

$\mathbb{R}/2\pi\mathbb{Z}$ sa mesure.

$$\begin{aligned}\gamma &= \mu((|\eta\rangle\,\hat{},|\beta\rangle)) \\ &= \mu((|\alpha\rangle\,\hat{},|\beta\rangle) - (|\alpha\rangle\,\hat{},|\eta\rangle)) \\ &= \frac{\pi}{2} - (2k+1)\theta'.\end{aligned}$$

Or on a choisi k tel que

$$(2k+1)\theta' \leq \frac{\pi}{2} < (2k+3)\theta'$$

Donc

$$\frac{\pi}{2} - (2k+1)\theta' < 2\theta'$$

donc

$$\gamma < 2\theta'.$$

9.2 La sesqui-linéarité du produit scalaire justifie le calcul suivant :

$$\begin{aligned}\| \, |\eta\rangle - |\beta\rangle \, \|^2 &= \| \, |\eta\rangle \, \|^2 + \| \, |\beta\rangle \, \|^2 - 2 \, \langle\beta|\eta\rangle \\ &= 1 + 1 - 2\cos(\gamma) \\ &= 2(1-\cos(\gamma)) \\ &= 4\sin^2(\gamma/2).\end{aligned}$$

9.3 En utilisant Q9.2 puis Q3 puis l'hypothèse de l' étape 3, cas 1 :

$$\| \, |\eta\rangle - |\beta\rangle \, \|^2 = 4\sin^2(\gamma/2) \leq 4\sin^2(\theta') = 4\frac{M}{N} \leq 4s.$$

10- Notons λ_x (resp. μ_x)la valeur propre de vecteur propre $|x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ (resp. $|x\rangle \, \frac{|0\rangle + |1\rangle}{\sqrt{2}}$).
10.1 Décomposons le vecteur$|\eta\rangle$ sur les sous-espaces propres de $\mathcal{M}$:

$$|\eta\rangle = \sum_{f(x)=0} \rho_x \cdot |x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} + \sum_{f(x)=1} \rho_x \cdot |x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} + \sum_{x\in\mathbb{B}^n} 0 \cdot |x\rangle \, \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$

avec

$$\sum_{f(x)=0} \rho_x \cdot |x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \cos(\pi/2-\gamma) \, |\alpha\rangle \, , \quad \sum_{f(x)=1} \rho_x \cdot |x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sin(\pi/2-\gamma) \, |\beta\rangle \, .$$

Le postulat de la mesure, en mécanique quantique entraîne que :

$$\Pr(\bigcup_{f(x)=0}\{\mathcal{M}=\lambda_x\})=\sum_{f(x)=0}\rho_x^2,\ \ \Pr(\bigcup_{f(x)=1}\{\mathcal{M}=\lambda_x\})=\sum_{f(x)=1}\rho_x^2,\ \ \Pr(\bigcup_{x\in\mathbb{B}^n}\{\mathcal{M}=\mu_x\})=0.$$

Donc

$$\begin{aligned}\Pr(\bigcup_{f(x)=0}\{\mathcal{M}=\lambda_x\}) &= \sum_{f(x)=0}\rho_x^2\\ &= \|\cos(\pi/2-\gamma)\,|\alpha\rangle\,\|^2\\ &= \sin^2(\gamma)\\ &\leq 4\sin^2(\gamma/2)\\ &\leq 4\frac{M}{N}\\ &\leq 4s\end{aligned}$$

et comme $\Pr(\bigcup_{x\in\mathbb{B}^n}\{\mathcal{M}=\mu_x\})=0$, la probabilité de l'événement comlémentaire des deux événements ci-dessus est $\geq(1-4s)$:

$$\Pr(\bigcup_{f(x)=1}\{\mathcal{M}=\lambda_x\})\geq(1-4s).$$

10.2 Si on répète r fois l'algorithme, la probabilité d'échouer (i.e. de ne pas obtenir une valeur x telle que $f(x)=1$) est :

$$p_r\leq(4s)^r$$

donc la probabilité de réussite est

$$1-p_r\geq 1-(4s)^r$$

Cette probabilité est supérieure ou égale à $1-\frac{1}{1000}$ si $(4s)^r\leq\frac{1}{1000}$; donc il suffit que

$$r\geq -3\frac{\ln(10)}{\ln(4s)}$$

pour $s=1/100$ on obtient $r=-3\frac{\ln(10)}{\ln(4\cdot 10^{-2})}$.
11- Par un raisonnement analogue à celui de la question 10.2 on obtient :

$$r\geq -3\frac{\ln(10)}{\ln(1-s)}$$

12- 12.1 On suit le même raisonnement quà la question 10, en remplaçant le vecteur $|\eta\rangle$ par le vecteur $|\psi\rangle$.

$$|\psi\rangle = \sum_{f(x)=0} \frac{1}{\sqrt{N}} \cdot |x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} + \sum_{f(x)=1} \frac{1}{\sqrt{N}} \cdot |x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} + \sum_{x \in \mathbb{B}^n} 0 \cdot |x\rangle \, \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Donc

$$\begin{aligned} \Pr(\bigcup_{f(x)=0} \{\mathcal{M} = \lambda_x\}) &= \sum_{f(x)=0} \frac{1}{N} \\ &= \frac{N-M}{N} \\ &\leq 1 - s. \end{aligned}$$

12.2 Si on répète r fois l'algorithme, la probabilité d'échouer (i.e. de ne pas obtenir une valeur x telle que $f(x) = 1$ est :

$$p_r \leq (1-s)^r$$

On obtient une probabilité de réussite supérieure ou égale à $1 - \frac{1}{1000}$ lorsque $(1-s)^r \leq \frac{1}{1000}$; donc il suffit que

$$r \geq -3 \frac{\ln(10)}{\ln(1-s)}$$

pour $s = 1/100$ on obtient $r = -3\frac{\ln(10)}{\ln(1-10^{-2})}$.
Remarque finale : Aussi bien dans le cas 1, que dans le cas 2, le nombre de rétitions de l'algorithme est constant. L'algorithme complet a donc la même complexité que la version de base de l'algorithme de Grover i.e. $O(\sqrt{N})$.