ENSEIRB-MATMECA
Option second semestre, 2011/2012

Information Quantique

Examen- 21 Mai 2012

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

Exercice 1 (/8 pts)

Circuits quantiques.

On a vu, lors du DM, que l'opérateur de Toffoli (quantique) est décomposable en un circuit n'utilisant que des portes à deux qbits. Cet exercice consiste à détailler cette construction puis à l'étendre à des opérateurs plus généraux.
On pose

$$\mathsf{N\hat{O}T} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

1- Donner explicitement une matrice unitaire R telle que $R^2 = \mathsf{N\hat{O}T}$,

On choisit maintenant une telle matrice unitaire R.
On définit, pour $1 \leq k \leq n$ et tout opérateur unitaire U sur $\mathcal{B}$, l'opérateur $\Lambda^k(U)$ sur $\mathcal{B}^{\otimes(k+1)}$ par :

$$\begin{aligned} \Lambda^k(U)\,|x_1,\ldots,x_k,x_{k+1}\rangle = &\quad |x_1,\ldots,x_k\rangle \otimes |x_{k+1}\rangle \qquad \text{si } x_1x_2\cdots x_k = 0 \\ = &\quad |x_1,\ldots,x_k\rangle \otimes U\,|x_{k+1}\rangle \qquad \text{si } x_1x_2\cdots x_k = 1 \end{aligned}$$

2- Vérifier que l'opérateur de Toffoli est égal à l'opérateur $\Lambda^2(\mathsf{N\hat{O}T})$.
3- On définit le circuit T sur 3 qbits :

$$T := \Lambda^1(R)[(2,3)]\mathsf{cN\hat{O}T}[(1,2)]\Lambda^1(R^{-1})[(2,3)]\mathsf{cN\hat{O}T}[(1,2)]\Lambda^1(R)[(1,3)]$$

(on utilise ici la notation du DM ; on peut aussi utiliser la figure 1 et raisonner sur des diagrammes de la même forme).
Montrer que ce circuit T calcule l'opérateur de Toffoli.
Indication : on pourra distinguer les quatre cas de figure $(x_1, x_2) = (0, 0)$, $(x_1, x_2) =$

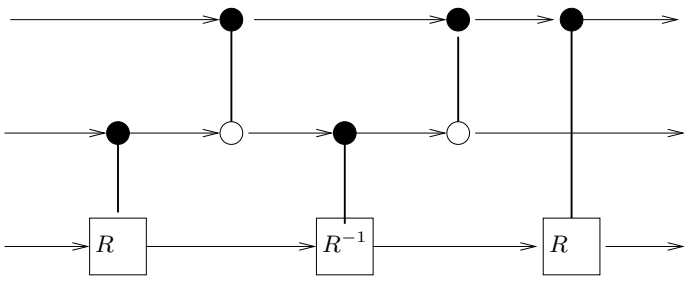

FIGURE 1 – Le circuit T

$(0,1)$, $(x_1,x_2)=(1,0)$, $(x_1,x_2)=(1,1)$ et vérifier que, dans chaque cas, $T\,|x_1,x_2,x_3\rangle = \mathsf{T\hat{O}F}\,|x_1,x_2,x_3\rangle$.
4- Soit $U:\mathcal{B}\to\mathcal{B}$ une application linéaire unitaire. Montrer que U a une racine carrée unitaire i.e. il existe une application linéaire unitaire $V:\mathcal{B}\to\mathcal{B}$ telle que $V^2=U$.
5- Donner un circuit C_U sur l'ensemble de portes $\{\mathsf{cN\hat{O}T}, \Lambda^1(V), \Lambda^1(V^{-1})\}$, qui calcule $\Lambda^2(U)$.
6- Soit $k\geq 1$.
6.1- Montrer que l'opérateur $\Lambda^k(U)$ est calculable par un circuit, (sans qbit auxiliaire) sur l'ensemble de portes $\{\mathsf{cN\hat{O}T}\}\cup\{\Lambda^1(W), W\in\mathsf{U}(2)\}$.
6.2 Préciser la longueur (i.e. le nombre de portes) du circuit proposé.

Exercice 2(/15 pts)
Algorithme de Grover

On s'intéresse au problème algorithmique suivant :
Données : un circuit quantique calculant une application $f:\mathbb{B}^n\to\mathbb{B}$ et le nombre M de vecteurs $x\in\mathbb{B}^n$ tels que $f(x)=1$.
Calculer : un vecteur $x\in\mathbb{B}^n$ tel que $f(x)=1$.
On a étudié en cours l'algorithme de Grover, qui résout ce problème dans le cas où $M=1$.
Le but de l'exercice est de comprendre comment on peut adapter l'algorithme de Grover au cas général (i.e. M entier quelconque, non-nul).
On note $N:=2^n$. On rappelle ci-dessous les étapes de l'algorithme de Grover, et on examine les modifications à apporter.
On dispose d'un circuit quantique qui calcule l'opérateur unitaire
(l'"oracle") $\mathrm{O}:\mathcal{B}^{\otimes(n+1)}\to\mathcal{B}^{\otimes(n+1)}$ tel que, pour tous $x\in\mathbb{B}^n, q\in\mathbb{B}$

$$|x\rangle\,|q\rangle \overset{\mathrm{O}}{\mapsto} |x\rangle\,|q\oplus f(x)\rangle$$

Étape 0 On initialise l'état du système à $(n+1)$ qbits à

$$|0^n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Étape 1 On applique n portes de Hadamard, en parallèle, aux n premiers qbits :

$$|0^n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \mapsto \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{B}^n} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |\psi\rangle$$

On pose

$$\begin{aligned} |\alpha\rangle &:= \frac{1}{\sqrt{N-M}} \sum_{f(x)=0} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ |\beta\rangle &:= \frac{1}{\sqrt{M}} \sum_{f(x)=1} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned}$$

1- Vérifier que les vecteurs $|\alpha\rangle, |\beta\rangle$ sont de norme 1 et sont orthogonaux.
2- Calculer les coefficients $c_\alpha, c_\beta \in \mathbb{R}$ tels que

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

On se place dans le sous-espace vectoriel réel P engendré par les vecteurs $|\alpha\rangle, |\beta\rangle$. On oriente ce plan en convenant que la base $(|\alpha\rangle, |\beta\rangle)$ est directe. Le produit scalaire (hermitien) restreint à ce sous-espace réel, lui confère une structure de plan euclidien.
3- Calculer la mesure θ' de l'angle $(|\alpha\rangle, |\psi\rangle)$.
Indication : on pourra évaluer $\sin(\theta')$ en fonction de N et M.
Étape 2
On applique l'oracle

$$|\psi\rangle \mapsto \mathrm{O}|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{B}^n} (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

4- Montrer que

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

On définit l'opérateur $S_0 : \mathcal{B}^{\otimes(n+1)} \to \mathcal{B}^{\otimes(n+1)}$ par :

$$\begin{aligned} S_0 : |0^n\rangle |y\rangle &\mapsto |0^n\rangle |y\rangle \quad \text{pour } y \in \{0,1\} \\ |x\rangle |y\rangle &\mapsto -|x\rangle |y\rangle \quad \text{pour } x \in \mathbb{B}^n, x \neq 0^n, y \in \{0,1\} \end{aligned}$$

5- Vérifer que S_0 est la symétrie orthogonale par rapport au plan (complexe) P_0 engendré par les vecteurs $|0^n\rangle\,|0\rangle\,, |0^n\rangle\,|1\rangle$.
6- On définit l'opérateur (sur $(n+1)$ qbits) :

$$S_\psi := (H^{\otimes n} \otimes \mathrm{Id}) S_0 (H^{\otimes n} \otimes \mathrm{Id})$$

Montrer que S_ψ est une symétrie orthogonale par rapport au plan (complexe) engendré par les vecteurs $|\psi\rangle\,, |\psi'\rangle$, où $|\psi'\rangle := \frac{1}{\sqrt{N}} \sum_{x\in\mathbb{B}^n} |x\rangle\, \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.
7- Montrer que chacun des opérateurs O, S_ψ stabilise le plan (réel) P (défini après la question 2).
Indication : il suffit de calculer les images de $|\alpha\rangle$ et de $|\psi\rangle$ par ces deux opérateurs.
On note $\tilde{S_\psi}$ (resp. $\tilde{\mathrm{O}}$) la restriction de S_ψ (resp. O) au plan P.
8-
8.1 Montrer que $\tilde{S_\psi}\tilde{\mathrm{O}}$ est une rotation de P.
8.2 Calculer une mesure θ de l'angle de la rotation $\tilde{S_\psi}\tilde{\mathrm{O}}$.
Indication : on pourra exprimer θ en fonction de θ'.

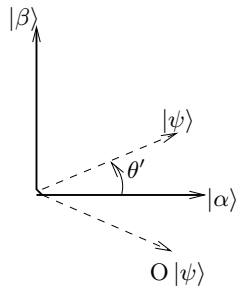

FIGURE 2 – Le plan P

Étape 3, cas 1
On suppose que

$$\frac{M}{N} \leq s \tag{1}$$

où s est un "seuil" que l'on a choisi "petit devant 1" ; pour fixer les idées, supposons que $s = \frac{1}{100}$.
On calcule un entier k tel que

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

On applique $(S_\psi \mathrm{O})^k$ au vecteur $|\psi\rangle$, on obtient le vecteur $|\eta\rangle$.
9-
9.1 Soit $\gamma \in [0, 2\pi[$ la mesure de l'angle entre $|\eta\rangle$ et $|\beta\rangle$; Vérifier que $0 \leq \gamma < 2\theta'$.
9.2 Montrer que $\| \, |\eta\rangle - |\beta\rangle \, \|^2 = 4\sin^2(\gamma/2)$.
9.3 En déduire que $\| \, |\eta\rangle - |\beta\rangle \, \|^2 \leq 4\frac{M}{N} \leq 4s$.
Pour simplifier le raisonnement, supposons que l'on connaisse une grandeur observable $\mathcal{M}$, associée à un opérateur hermitien M, sur $\mathcal{B}^{\otimes(n+1)}$, dont les vecteurs propres sont les 2^{n+1} vecteurs de la base

$$|x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}}, |x\rangle \, \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

pour $x \in \mathbb{B}^n$ et dont les valeurs propres soient toutes distinctes. Notons λ_x la valeur propre de vecteur propre $|x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.
10- On effectue une mesure de l'observable $\mathcal{M}$ sur le vecteur $|\eta\rangle$. Avec quelle probabilité le résultat de la mesure est-il une des valeurs propres

$$\lambda_x \text{ avec } f(x) = 1?$$

10.1 Montrer que cette probabilité est supérieure ou égale à $(1 - 4s)$.
10.2 Combien de répétitions de cet algorithme quantique sont nécessaires, pour obtenir un vecteur $x \in \mathbb{B}^n$, tel que $f(x) = 1$, avec une probabilité $\geq 1 - \frac{1}{1000}$?
Étape 3, cas 2
On suppose maintenant que

$$\frac{M}{N} > s. \tag{2}$$

et l'on tire aléatoirement un vecteur $x \in \mathbb{B}^n$.
La probabilité d'obtenir, en un seul tirage, un vecteur $x \in \mathbb{B}^n$, tel que $f(x) = 1$ vaut $\frac{M}{N} > s$.
11- Combien de tirages (indépendants) sont nécessaires, pour obtenir un vecteur $x \in \mathbb{B}^n$, tel que $f(x) = 1$, avec une probabilité $\geq 1 - \frac{1}{1000}$?
Par souci d'uniformité, on souhaite traiter le cas 2, comme le cas 1, par un algorithme quantique.
On mesure donc l'observable $\mathcal{M}$ directement sur le vecteur $|\psi\rangle$.
12- 12.1 Avec quelle probabilité le résultat de la mesure est-il une des valeurs propres

$$\lambda_x \text{ avec } f(x) = 1?$$

12.2 Combien de répétitions de cet algorithme quantique sont nécessaires, pour obtenir un vecteur $x \in \mathbb{B}^n$, tel que $f(x) = 1$, avec une probabilité $\geq 1 - \frac{1}{1000}$?