ENSEIRB-MATMECA
Option second semestre, 2012/2013

Information Quantique

Examen- 27 Mai 2013

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 (/20 pts)

Problème du sous-groupe caché.

L'exercice consiste à généraliser l'algorithme de Simon au calcul du *groupe des périodes* d'une application f de $(\mathbb{Z}/2\mathbb{Z})^n$ dans lui-même. On note $G := (\mathbb{Z}/2\mathbb{Z})^n$ le produit direct du groupe additif $(\mathbb{Z}/2\mathbb{Z}, \oplus)$ par lui-même (avec n facteurs $\mathbb{Z}/2\mathbb{Z}$). Autrement dit, la loi de groupe $\oplus$ est définie par : pour tous $x_0, \ldots, x_i, \ldots, x_{n-1}, y_0, \ldots, y_i, \ldots, y_{n-1}$ éléments de $\mathbb{Z}/2\mathbb{Z}$,

$$(x_0, \ldots, x_i, \ldots, x_{n-1}) \oplus (y_0, \ldots, y_i, \ldots, y_{n-1}) := (x_0 \oplus y_0, \ldots, x_i \oplus y_i, \ldots, x_{n-1} \oplus y_{n-1}).$$

Exemple :
Pour $n = 3$ on a $G = \{(x_0, x_1, x_2) \mid x_0, x_1, x_2 \in \mathbb{Z}/2\mathbb{Z}\}$, $\mathrm{Card}(G) = 2^3$,

$$(0,1,0) \oplus (1,0,1) = (1,1,1), \quad (0,1,1) \oplus (1,0,1) = (1,1,0), \quad (0,1,0) \oplus (0,1,0) = (0,0,0).$$

Soit $f : G \to G$ une application ayant la propriété de *périodicité* suivante : il existe un sous-groupe D de G, tel que

$$\forall x, y \in G, \quad (f(x) = f(y) \Leftrightarrow y - x \in D). \tag{1}$$

Tout sous-groupe D ayant la propriété (1) est appelé *sous-groupe des périodes* de f. On vérifie aisément que, f étant donnée, si un tel sous-groupe existe, il est unique.
Exemple :
Prenons $n = 3$ et $f(x_0, x_1, x_2) := (0, x_0 \oplus 1, x_0 \oplus 1)$.
Q1-Vérifier que, dans cet exemple,

$$D := \{(0,0,0), (0,0,1), (0,1,0), (0,1,1)\}$$

est le sous-groupe des périodes de f.
Comme d' habitude, on code l'élément $x = (x_0, \ldots, x_i, \ldots, x_{n-1})$ de G par le vecteur unitaire $|x\rangle := |x_0\rangle \otimes \ldots |x_i\rangle \ldots \otimes |x_{n-1}\rangle$ de $\mathcal{B}^{\otimes n}$.
Q2- Montrer que, pour tout $x \in G$

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in G} (-1)^{x \cdot z} |z\rangle$$

où $x \cdot z = x_0 z_0 \oplus x_1 z_1 \oplus \cdots \oplus x_{n-1} z_{n-1}$.

Q3- On dispose d'une boite noire U_f qui réalise $|x\rangle |y\rangle \overset{U_f}{\to} |x\rangle |y \oplus f(x)\rangle$ où $x \in G, y \in G$ et $f(x) \in G$. On réalise le circuit schématisé sur la figure 1.

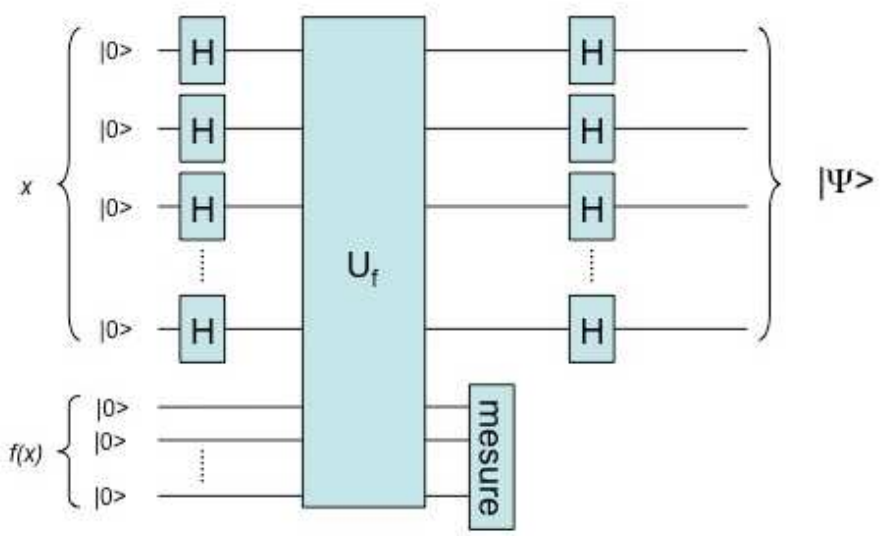

FIGURE 1 – Le circuit.

(a) Montrer que, juste avant la mesure, l'état du système est

$$\frac{1}{\sqrt{2^n}} \sum_{x \in G} |x\rangle \otimes |f(x)\rangle$$

(b) L'état du second registre après la mesure est $|w\rangle$ (où $w \in G$). Soit $\hat{x} \in G$ tel que : $f(\hat{x}) = w$. Exprimer l'état du système après cette mesure.

Q4- Exprimer, le plus simplement possible, l'ensemble $f^{-1}(w)$ à partir de $\hat{x}$ et de D. En déduire que $\mathrm{Card}(f^{-1}(w)) = \mathrm{Card}(D)$.
Q5- Après la (deuxième) transformation de Hadamard, l'état du système est de la forme

$$\sum_{z\in G} c(z)\,|z\rangle \otimes |w\rangle$$

où chaque $c(z)$ est un nombre complexe.
Montrer que

$$c(z) = \frac{1}{\sqrt{\mathrm{Card}(D)}} \sum_{x\in f^{-1}(w)} \langle z|\, H^{\otimes n}\, |x\rangle$$

Q6- En utilisant la question Q2, en déduire que

$$c(z) = \frac{1}{\sqrt{\mathrm{Card}(D)\mathrm{Card}(G)}} \sum_{x\in f^{-1}(w)} (-1)^{x\cdot z}$$

Q7- Montrer que $c(z) = \frac{1}{\sqrt{\mathrm{Card}(D)\mathrm{Card}(G)}} \sum_{d\in D} (-1)^{\hat{x}\cdot z \oplus d\cdot z}$.
Q8- On note $D^\perp := \{g \in G \mid \forall d \in D, d\cdot g = 0\}$. Que vaut $c(z)$ pour $z \in D^\perp$? pour $z \notin D^\perp$?
Q9- En conclure que l'état final $|\psi\rangle \otimes |w\rangle$ appartient au sous-espace vectoriel engendré par $\{|z\rangle \otimes |w\rangle \mid z \in D^\perp\}$.
Q10- On réalise alors une mesure du premier registre et on note le résultat z_1 ; on réinitialise le système et on reparcourt tout le circuit, puis on effectue une mesure du premier registre et on note le résultat z_2 ; on répète cette opération ℓ fois pour obtenir un ensemble de mesures $\{z_1, z_2, ...z_\ell\}$. Évaluons la probabilité que ces ℓ éléments de G engendrent $D^\perp$.
a- Combien $D^\perp$ a-t-il de sous-groupes de cardinal 2 ?
b- Combien $D^\perp$ a-t-il de sous-groupes de cardinal $\frac{\mathrm{Card}(D^\perp)}{2}$? (On pourra utiliser l'orthogonalité dans $D^\perp$, vu comme un espace vectoriel sur le corps $\mathbb{Z}/2\mathbb{Z}$)
On note $\langle z_1, z_2, ...z_\ell\rangle$ le sous-groupe de $D^\perp$ engendré par $\{z_1, z_2, ...z_\ell\}$.
c- Montrer que, pour chaque sous-groupe Y de $D^\perp$, de cardinal $\frac{\mathrm{Card}(D^\perp)}{2}$, la probabilité que $\langle z_1, z_2, ...z_\ell\rangle \subseteq Y$ est $\leq \frac{1}{2^\ell}$
d- Montrer que la probabilité que $\langle z_1, z_2, ...z_\ell\rangle = D^\perp$ est $\geq 1 - \frac{\mathrm{Card}(D^\perp)}{2^\ell}$
Q11- Comment peut-on calculer D à partir de $D^\perp$? Combien d'évaluations de f faut-il faire pour obtenir D avec une probabilité $\geq \frac{99}{100}$?

Exercice 2(/15 pts)

Jeu de Zeilinger.

Une équipe de trois joueurs Anne (A), Benoît (B) et Charles (C), est opposée à un arbitre R. Chaque partie se déroule comme suit :
Phase 0- A,B,C communiquent librement : ils se mettent d'accord sur une stratégie et éventuellement un vecteur $\vec{\lambda}$ qu'ils peuvent utiliser dans leur stratégie.
Phase 1- R choisit un triplet de questions $(r, s, t) \in \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$ R envoie la question r à Anne, la question s à Benoît et la question t à Charles (chaque joueur ne connaît que la question qu'il reçoit de R).
Phase 2- Anne répond par un booléen $a \in \{0,1\}$, Benoît par $b \in \{0,1\}$ et Charles par $c \in \{0,1\}$.
Phase 3- L'équipe ABC reçoit un gain de 1 dans les cas suivants

r	s	t	$a \oplus b \oplus c$	gain
0	0	0	0	1
0	1	1	1	1
1	0	1	1	1
1	1	0	1	1

et perd i.e. gagne -1, dans tout autre cas. Dans tous les scénarios examinés ci-dessous, A,B,C ne sont pas autorisés à communiquer entre eux au cours des phases 1,2,3 du jeu ;
Q1- Montrer que l' équipe ABC n'a pas de stratégie déterministe qui gagne sur toute question de R.
Q2- On suppose que R tire ses questions de façon aléatoire, uniforme. Quelle est l'espérance de gain maximale de ABC, avec une stratégie déterministe ?
Q3- Supposons maintenant que A,B,C partagent trois qbits intriqués, dans l'état

$$|\psi\rangle := \frac{1}{2}|000\rangle - \frac{1}{2}|011\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle .$$

Ils choisissent la stratégie (quantique) suivante :
- sur la question $q = 1$ (resp. $q = 0$), le joueur applique H (resp. Id) à son qbit.
- chaque joueur "mesure son qbit dans la base standard" et renvoie à R le résultat de cette mesure.
Q3.1 Quel est le gain de ABC sur la question 000 ?
Q3.2 Quel est le gain de ABC sur la question 011 ?
Aide : On pourra calculer le vecteur d'état $|\psi'\rangle$ obtenu par les joueurs A,B,C en appliquant chacun leur transformation unitaire sur leur qbit, puis en déduire les réponses possibles de ABC.
Q3.3 Quel est le gain moyen de ABC (avec cette stratégie) ?