ENSEIRB-MATMECA, 2ième année
Option second semestre, 2016/2017

Information Quantique

Examen du 19 Mai 2017

Durée : 2H
Documents autorisés : tous documents autorisés.
Indications : les exercices sont indépendants.
Notation : le barème est indicatif.

Exercice 1 (/10 pts)

Circuits réversibles/quantiques.

On fixe dans tout l'exercice un entier $n \geq 1$. On désigne par $\mathbb{D}_n$ l'ensemble des mots de longueur n sur $\{0,1\}$:

$$\mathbb{D}_n := \{0,1\}^n.$$

Cet ensemble est muni de plusieurs structures algébriques.
Groupe additif $((\mathbb{Z}/2\mathbb{Z})^n, \oplus_n)$: si $x = (x_1, \ldots, x_k, \ldots, x_n), y = (y_1, \ldots, y_k, \ldots, y_n)$ alors

$$x \oplus_n y = (x_1 \oplus y_1, \ldots, x_k \oplus y_k, \ldots, x_n \oplus y_n),$$

où $\oplus$ dénote l'addition dans $\mathbb{Z}/2\mathbb{Z}$.
Anneau des entiers modulo 2^n : $(\mathbb{Z}/2^n\mathbb{Z}, +_A, \cdot)$: si $x = (x_1, \ldots, x_k, \ldots, x_n), y = (y_1, \ldots, y_k, \ldots, y_n), z = (z_1, \ldots, z_k, \ldots, z_n)$, alors

$$x +_A y = z$$

signifie

$$\sum_{k=1}^{n} x_k 2^{n-k} + \sum_{k=1}^{n} y_k 2^{n-k} \equiv \sum_{k=1}^{n} z_k 2^{n-k} \pmod{2^n}.$$

et

$$x \cdot y = z$$

signifie

$$(\sum_{k=1}^{n} x_k 2^{n-k}) \cdot (\sum_{k=1}^{n} y_k 2^{n-k}) \equiv \sum_{k=1}^{n} z_k 2^{n-k} \pmod{2^n}.$$

On réserve la notation + pour l'addition dans $\mathbb{Z}$. Pour toute application $f : \mathbb{D}_n \to \mathbb{D}_n$ on définit $f_+ : \mathbb{D}_n \times \mathbb{D}_n \to \mathbb{D}_n \times \mathbb{D}_n$ par : pour tous $x \in \mathbb{D}_n, y \in \mathbb{D}_n$,

$$f_+(x, y) := (x, y +_A f(x)).$$

On définit aussi $f_\oplus : \mathbb{D}_n \times \mathbb{D}_n \to \mathbb{D}_n \times \mathbb{D}_n$: pour tous $x \in \mathbb{D}_n, y \in \mathbb{D}_n$,

$$f_\oplus(x, y) := (x, y \oplus_n f(x)).$$

1- Montrer que, pour toute application f, les applications $f_+, f_\oplus$ sont des bijections de $\mathbb{D}_n \times \mathbb{D}_n$ dans lui-même.
On considère l'ensemble de portes booléennes réversibles

$$\mathcal{G} := \{\mathsf{NOT}, \mathsf{cNOT}, \mathsf{SWAP}, \mathsf{TOF}, \mathsf{OR}_\oplus\}.$$

2- Montrer que, si C est un circuit sur $\mathcal{G}$ qui calcule une bijection $c : \mathbb{D}_\ell \to \mathbb{D}_\ell$, alors on peut construire un circuit $\bar{C}$ sur $\mathcal{G}$ qui calcule c^{-1}. Autrement dit, pour toutes suites de bits $s, t \in \mathbb{D}_\ell$:

$$C(s) = t \Leftrightarrow \bar{C}(t) = s.$$

Aide : vérifier que chaque porte de $\mathcal{G}$ est involutive.

On suppose qu'un circuit réversible C sur $\mathcal{G}$, "calcule" f au sens suivant : pour tout $x \in \mathbb{D}_n$,

$$C(x, 0^m) = (f(x), g(x))$$

i.e. le circuit C prend en entrée les n bits de x et m bits de valeur 0 et donne en sortie $f(x)$ suivi d'une suite $g(x)$ de m bits. Le mot $g(x) \in \mathbb{D}_m$ est vu comme un "déchet" du calcul, qui a indûment remplacé les zéros des bits auxiliaires.

On cherche à construire un circuit C' sur $\mathcal{G}$ tel que, pour tous $x, y \in \mathbb{D}_n$

$$C'(x, y, 0^m) = (x, y \oplus_n f(x), 0^m) \tag{1}$$

ce qui correspondra à un calcul "sans déchet" (donc conforme à la définition vue en cours de l'usage des bits auxiliaires).

3- Construire un circuit $\mathsf{ID}_\oplus$ sur $\mathcal{G}$ tel que, pour tous $x \in \mathbb{D}_n, y \in \mathbb{D}_n$,

$$\mathsf{ID}_\oplus(x, y) = (x, x \oplus_n y).$$

4- 4.1 En utilisant les circuits $C, \bar{C}$ et $\mathsf{ID}_\oplus$, construire un circuit C' vérifiant l'équation (1).

4.2 Majorer le nombre de portes de C' en fonction du nombre de portes de C.

Soit $f : \mathbb{D}_n \to \mathbb{D}_n$ une bijection et C, D deux circuits sur $\mathcal{G}$ tels que : C calcule $f_\oplus$ (sans "déchet") et D calcule $(f^{-1})_\oplus$ (sans "déchet") i.e. :

$$C(x, y, 0^m) = (x, y \oplus_n f(x), 0^m), \quad D(x, y, 0^m) = (x, y \oplus_n f^{-1}(x), 0^m).$$

5- Construire un circuit E sur $\mathcal{G}$, éventuellement avec des bits auxiliaires, qui calcule f sans déchet, i.e. il existe un entier $\ell \geq 0$ tel que, pour tout $x \in \mathbb{D}_n$,

$$E(x, 0^\ell) = (f(x), 0^\ell).$$

Soit $f : \mathbb{D}_n \to \mathbb{D}_n$ une bijection telle que chacune des deux fonctions f_+ (resp. f_+^{-1}) est calculée par un circuit F (resp. G) (avec "déchet").
6- Construire un circuit H sur $\mathcal{G}$, éventuellement avec des bits auxiliaires, qui calcule f sans déchet, i.e. il existe un entier $\ell \geq 0$ et pour tout $x \in \mathbb{D}_n$,

$$H(x, 0^\ell) = (f(x), 0^\ell).$$

Aide : on trouvera d'abord des circuits qui calculent, avec déchet, les fonctions f, f^{-1}, puis on utilisera les questions qui précédent.

On cherche maintenant à construire, pour tout mot a qui représente un entier impair, un circuit sur $\mathcal{G}$ qui calcule $x \mapsto a \cdot x$.

7- Construire un circuit AD_1 sur $\mathcal{G}$, (éventuellement avec bits auxilaires, et déchet) tel que, pour tous $r, x, y \in \mathbb{B}$

$$AD_1(r, x, y) = (r', x, x \oplus y)$$

où $r' = 1$ ssi $x + y + r \geq 2$.
Autrement dit : AD_1 est un additionneur, qui prend en entrée les bits x, y, et la retenue r et fournit en sortie le résultat $x \oplus y$ et la nouvelle retenue r'.
8- Construire un circuit AD sur $\mathcal{G}$, (avec bits auxiliaires, et déchet) tel que, pour tous $x, y \in \mathbb{D}_n$,

$$AD(x, y) = (x, x +_A y)$$

Pour tout entier $p \in [0, 2^n - 1]$, on note $\mu(p) \in \mathbb{D}_n$ l'unique mot $\mu(p) := \mu_1 \dots \mu_k \dots \mu_n$ qui dénote p en base 2 i.e. tel que $\sum_{k=1}^n \mu_k \cdot 2^{n-k} = p$.
Par exemple : si $n = 4$

$$\mu(2) = 0010, \quad \mu(5) = 0101, \quad \mu(8) = 1000, \quad \mu(9) = 1001$$

et si $n = 5$

$$\mu(2) = 00010, \quad \mu(5) = 00101, \quad \mu(8) = 01000, \quad \mu(9) = 01001.$$

9- Construire un circuit $\mathsf{MUL2}$ sur $\mathcal{G}$, (avec bits auxiliaires, et déchet) tel que, pour tous $x, y \in \mathbb{D}_n$

$$\mathsf{MUL2}(x, y) = (x, x +_A \mu(2) \cdot y)$$

10- Pour tout entier $k \in [0, n-1]$, construire un circuit $\mathsf{MUL2}_k$ sur $\mathcal{G}$, (avec bits auxiliaires, et déchet) tel que, pour tous $x, y \in \mathbb{D}_n$

$$\mathsf{MUL2}_k(x, y) = (x, x +_A \mu(2^k) \cdot y)$$

11- Pour tout entier $a \in [0, 2^n - 1]$, construire un circuit M_a sur $\mathcal{G}$, (avec bits auxilaires, et déchet) tel que, pour tous $x, y \in \mathbb{D}_n$

$$\mathsf{M}_a(x, y) = (x, x +_A a \cdot y)$$

12- Soit $a \in \mathbb{D}_n$, représentant (en base 2) un entier impair. Construire un circuit P_a sur $\mathcal{G}$, avec ℓ bits auxiliaires, *sans déchet*, qui calcule la bijection $x \mapsto a \cdot x$ i.e.

$$\mathsf{P}_a(x, 0^\ell) = (a \cdot x, 0^\ell).$$

13- Construire un circuit quantique sur l'ensemble des portes

$$\hat{\mathcal{G}} := \{\hat{\mathsf{NOT}}, \hat{\mathsf{cNOT}}, \hat{\mathsf{SWAP}}, \hat{\mathsf{TOF}}, \hat{\mathsf{OR}}_\oplus\}.$$

qui calcule (avec des q-bits auxiliaires, sans déchet)

$$|x\rangle \mapsto |a \cdot x\rangle .$$

Majorer la taille de ce circuit en fonction de n.

Formellement, un circuit quantique sur ℓ qbits est un mot sur l'alphabet $\{\mathrm{I}_{2^p} \otimes g \otimes \mathrm{I}_{2^q} \mid p \leq \ell, q \leq \ell, g \in \hat{\mathcal{G}}\}$.

14- Décrire un algorithme classique qui résout le problème suivant
<u>donnée</u> : une suite a de n bits représentant un entier impair
<u>sortie</u> : un circuit quantique, sur $(m+n)$ qbits (n qbits d'entrée-sortie et m qbits auxiliaires) qui calcule $|x\rangle \mapsto |a \cdot x\rangle$.
Quelle est la complexité de cet algorithme ? (On s'efforcera de donner un algorithme de complexité aussi petite que possible).

Exercice 2(/10 pts)
Protocole de Bennett-Brassard 1984.

On reprend le protocole quantique BB84 de définition d'une clé secrète.
On fixe une base orthonormée $|x\rangle, |y\rangle$ du plan ; nous noterons $\oplus$ cette base.
On considère aussi la base $|x'\rangle, |y'\rangle$ définie par

$$|x'\rangle := \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle), \quad |y'\rangle := \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle).$$

Nous noterons $\otimes$ cette base.
A (Alice) et B (Bob) utilisent ces deux bases pour encoder et décoder des bits, comme vu en cours.
On note B_θ la base $|x_\theta\rangle, |y_\theta\rangle$ définie par

$$|x_\theta\rangle := \cos(\theta)\,|x\rangle - \sin(\theta)\,|y\rangle\,, \quad |y_\theta\rangle := \sin(\theta)\,|x\rangle + \cos(\theta)\,|y\rangle$$

autrement dit, $(|x\rangle, |y\rangle)$ est l'image de $(|x_\theta\rangle, |y_\theta\rangle)$ par une rotation d'angle θ. Alice tire aléatoirement un bit $a \in \{0, 1\}$. Elle l'encode dans un qbit en

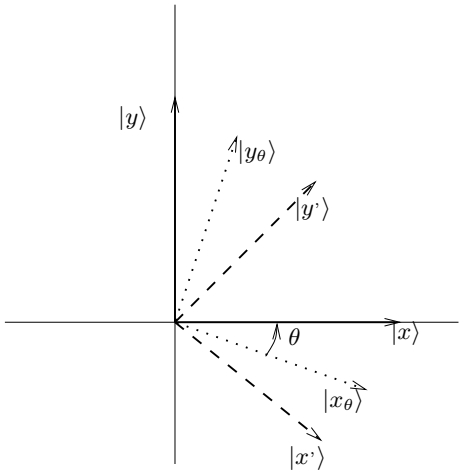

FIGURE 1 – Bases $\oplus$,$\otimes$,$(|x_\theta\rangle, |y_\theta\rangle)$.

utilisant soit la base $\oplus$, soit la base $\otimes$.
E (Eve) utilise la stratégie d'interception suivante :
- elle mesure le qbit (envoyé par A) dans la base B_θ ;
- si elle projette le qbit dans $|x_\theta\rangle$, elle déchiffre $e := 0$, si elle projette le qbit dans $|y_\theta\rangle$, elle déchiffre $e := 1$,

- elle renvoie à B le qbit (dans l'état où il se trouve après la mesure).
Puis B mesure le qbit envoyé par E, en utilisant soit la base $\oplus$, soit la base $\otimes$: il obtient $b \in \{0, 1\}$.
Revoyons tout d'abord quelle est la probabilité p pour Eve de déchiffrer correctement le bit de A. On distingue plusieurs cas.
1- A encode $a = 0$ avec la base $\oplus$.
Montrer que $p = \cos^2(\theta)$.
2- A encode $a = 1$ avec la base $\oplus$.
Montrer que $p = \cos^2(\theta)$.
3- A encode $a = 0$ avec la base $\otimes$.
Montrer que $p = \frac{1}{\sqrt{2}}(\cos(\theta) + \sin(\theta))^2$.
4- A encode $a = 1$ avec la base $\otimes$.
Montrer que $p = \frac{1}{\sqrt{2}}(\cos(\theta) + \sin(\theta))^2$.
5- A tire aléatoirement a et la base utilisée, suivant une loi uniforme, et ces deux tirages sont indépendants. En déduire que la probabilité que E déchiffre correctement le bit envoyé par A est :

$$\frac{1}{4}[2 + \sqrt{2}\cos(2\theta - \frac{\pi}{4})]$$

6- Pour quelles valeurs de θ cette probabilité est-elle maximale ?

On s'intéresse maintenant à la probabilité que E *ne soit pas détectée* par A, B. On suppose que le bit intercepté fait partie du lot de bits où A,B utilisent la *même base* et que A,B sacrifient à la sécurité :
si $a \neq b$ alors E est détectée, sinon E n'est pas détectée.

7- A envoie 0 dans la base $\oplus$.
Montrer que la probabilité que ($e = 0$ et $b = 0$) vaut $\cos^2(\theta) \cdot \cos(\theta)^2$
et la probabilité que ($e = 1$ et $b = 0$) vaut $\sin^2(\theta) \cdot \sin^2(\theta)$
8- A envoie 1 dans la base $\oplus$.
Montrer que la probabilité que ($e = 1$ et $b = 1$) vaut $\cos^2(\theta) \cdot \cos^2(\theta)$
et la probabilité que ($e = 0$ et $b = 1$) vaut $\sin^2(\theta) \cdot \sin^2(\theta)$
9- A envoie 0 dans la base $\otimes$.
Exprimer la probabilité que ($e = 0$ et $b = 0$), puis la probabilité que ($e = 1$ et $b = 0$).
10- A envoie 1 dans la base $\otimes$.
Exprimer la probabilité que ($e = 1$ et $b = 1$), puis la probabilité que ($e = 0$ et $b = 1$).
11- En déduire que la probabilité que E ne soit pas détectée est une combi-

naison linéaire

$$c_1 \cos^4(\theta) + c_2 \sin^4(\theta) + c_3 \cos^4(\frac{\pi}{4} - \theta) + c_4 \sin^4(\frac{\pi}{4} - \theta)$$

avec des coefficients rationnels c_1, c_2, c_3, c_4 que l'on précisera.
On définit la fonction $F : \mathbb{R} \to \mathbb{R}$ par

$$F(\theta) := \cos^4(\theta) + \sin^4(\theta).$$

12- Montrer que

$$\forall \theta \in \mathbb{R}, F(\theta) = \frac{1}{4}[3 + 2\cos(4\theta)].$$

13- 13.1 En déduire une expression simple de la probabilité que E ne soit pas détectée.
13.2 Pour quelles valeurs de θ cette probabilité est-elle maximale ?
14- E souhaite simultanément *maximiser* sa probabilité de *déchiffrer correctement* et sa probabilité de *ne pas être détectée*. Peut-elle atteindre cet objectif ? Si oui, quelle est alors sa probabilité de ne pas être détectée ?