Calcul Quantique Jeudi 3 Mai 2018

Midterm Solution

Exercice 1 *Réalisation de la porte SWAP (5 points)*

La porte est importante car elle permet d'échanger les q-bits dans un circuit. Elle est définie dans la base computationelle constituée des vecteurs $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$.

$$\mathrm{SWAP}\,|x\rangle \otimes |y\rangle = |y\rangle \otimes |x\rangle\,, \qquad x, y \in \{0, 1\}$$

(a) Démontrez que cette opération est unitaire.

(b) Donnez sa matrice correspondante en notation de Dirac et sous forme de tableau matriciel.

(c) Proposez un circuit quantique à l'aide de 3 portes Control-NOT qui réalise le SWAP.

Solution pour l'exercice 1 :

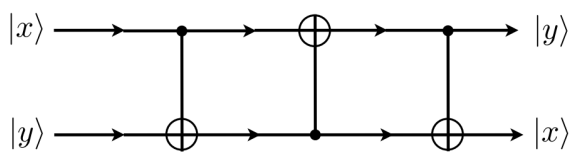
(a)

$$\langle x'| \otimes \langle y'|\,\mathrm{SWAP}^\dagger \mathrm{SWAP}\,|x\rangle \otimes |y\rangle = (\langle y'| \otimes \langle x'|)(|y\rangle \otimes |x\rangle) = \delta_{y',y}\delta_{x',x}$$

(b)

$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

(c) .



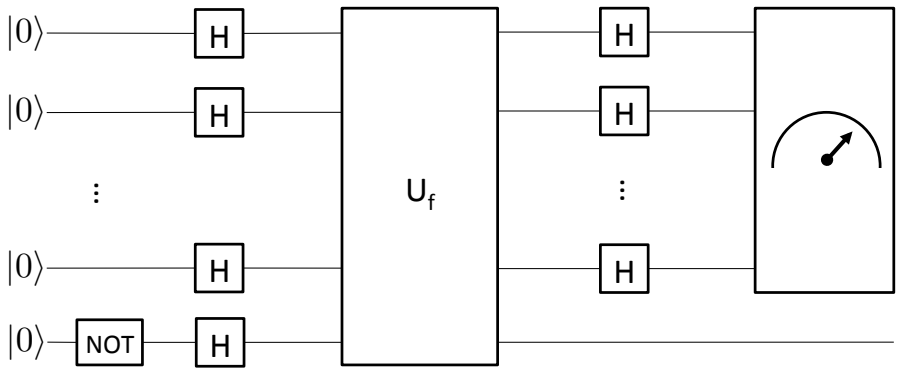
Exercice 2 *Algorithme de Bernstein-Vazirani (10 points)*

En 1993 E. Bernstein et U. Vazirani (Proc, 25th Annual ACM Symposium on the Theory of Computing, ACM Press, NY p11-20) formulèrent le problème suivant.

Soit $\underline{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$ des vecteurs binaires à n composantes. On se donne un "oracle" qui calcule

$$f(\underline{x}) = b \oplus (\underline{a} \cdot \underline{x}) \mod 2$$

où $b \in \mathbb{F}_2$ et $\underline{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_2^n$ et $\underline{a} \cdot \underline{x} = \sum_{i=1}^n a_i x_i$. Le but est de calculer $\underline{a}$ en posant le moins de questions possibles à l'oracle : pour fixer les idées on suppose b connu et $\underline{a}$ inconnu. On considère le circuit de Deutsch et Josza :



Rappel : $U_f \, |x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes |y\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes |y \oplus f(\underline{x})\rangle$

(a) Calculez l'état de sortie du circuit - juste avant l'appareil de mesure - quand tous les qubits d'entrée sont dans l'état $|0\rangle$. Il est utile de remarquer que $|f(\underline{x})\rangle - |1 \oplus f(\underline{x})\rangle = (-1)^{f(\underline{x})}(|0\rangle - |1\rangle)$.

(b) Grâce à l'appareil de mesure on fait *une seule* mesure dans la base computationelle des n premiers qubits de sortie du circuit. Montrer que cela suffit à déterminer le vecteur $\underline{a}$ avec probabilité 1.

(c) A-t-on besoin de savoir la valeur de b pour le succès de l'algorithme ? Si celle-ci n'est pas connue, est-ce que cet algorithme permet de la déterminer ? Justifiez.

Solution pour l'exercice 2 :

(a) L'état apès le premier ensemble des portes H :

$$\begin{aligned} H\,|0\rangle \otimes \cdots \otimes H\,|0\rangle \otimes H\,|1\rangle &= \frac{1}{2^{n/2}}\big((|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)\big) \otimes \frac{1}{\sqrt{2}}((|0\rangle - |1\rangle)) \\ &= \frac{1}{2^{n/2}} \sum_{\underline{x} \in \{0,1\}^n} |x_1, \ldots, x_n\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

L'état apès le U_f :

$$\frac{1}{2^{n/2}} \sum_{\underline{x}\in\{0,1\}^n} |x_1,\ldots,x_n\rangle \otimes \frac{1}{\sqrt{2}}(|f(\underline{x})\rangle - |1 \oplus f(\underline{x})\rangle)$$
$$= \frac{1}{2^{n/2}} \sum_{\underline{x}\in\{0,1\}^n} |x_1,\ldots,x_n\rangle \otimes \frac{1}{\sqrt{2}}(-1)^{f(\underline{x})}(|0\rangle - |1\rangle)$$

L'état après le 2nd ensemble des portes H :

$$\frac{1}{2^{n/2}} \sum_{\underline{x}\in\{0,1\}^n} (-1)^{f(\underline{x})} H\otimes\cdots\otimes H\,|x_1,\ldots,x_n\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$= \frac{1}{2^{n/2}} \sum_{\underline{x}\in\{0,1\}^n} (-1)^{f(\underline{x})}\big(\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)\otimes\cdots\otimes\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_n}|1\rangle)\big)\otimes\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$= \frac{1}{2^n} \sum_{\underline{x}\in\{0,1\}^n} (-1)^{f(\underline{x})} \sum_{y\in\{0,1\}^n} (-1)^{\underline{x}\cdot\underline{y}}\,|y_1,\ldots,y_n\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$$
$$= \frac{1}{2^n} \sum_{\underline{x}\in\{0,1\}^n} \sum_{y\in\{0,1\}^n} (-1)^{b+\underline{a}\cdot\underline{x}+\underline{x}\cdot\underline{y}}\,|y_1,\ldots,y_n\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$$

(b) La probabilité d'observer l'état des n premiers qubits $|y_1,\ldots,y_n\rangle$ dans la mesure est

$$\text{Prob}(|y_1,\ldots,y_n\rangle) = \frac{1}{2^{2n}}\Big|\sum_{\underline{x}\in\{0,1\}^n}(-1)^{(\underline{a}+\underline{y})\cdot\underline{x}}\Big|^2 = \begin{cases}1 & \text{si } \underline{a}=\underline{y}\\ 0 & \text{sinon}\end{cases}$$

Donc on toujours observe $|y_1,\ldots,y_n\rangle = |a_1,\ldots,a_n\rangle$.

(c) De la probabilité en (b), l'algorithme est independant de b.

Exercice 3 *Estimation de phase basée sur la transformée de Fourier quantique (10 points)*

Soit U une matrice unitaire $2^n \times 2^n$ (ici $n \geq 1$) possédant un vecteur propre $|u\rangle$ avec valeur propre $e^{2\pi i\varphi}$. C'est à dire :

$$U|u\rangle = e^{2\pi i\varphi}|u\rangle.$$

On suppose

$$\varphi = \frac{\varphi_1}{2} + \frac{\varphi_0}{4}$$

avec $\varphi_1, \varphi_0 \in \{0,1\}$ binaires. Dans ce problème on étudie un "algorithme d'estimation de phase" qui permet de découvrir φ en supposant le vecteur propre $|u\rangle$ connu.

On rappelle que la transformée de Fourier quantique agissant sur deux qubits est définie par

$$QFT|x_1,x_0\rangle = \frac{1}{2}\sum_{y_0,y_1\in\{0,1\}} e^{\frac{2\pi i}{4}(2x_1+x_0)(2y_1+y_0)}|y_1,y_0\rangle$$

où ici $x_1, x_0 \in \{0,1\}$. Nous définissons aussi les opérations (controllées) suivantes qui agissent sur $2+n$ qubits (ici $x, y \in \{0,1\}$ et $|\psi\rangle \in \mathbb{C}^{\otimes n}$)

$$R_1\,|x\rangle\otimes|y\rangle\otimes|\psi\rangle = |x\rangle\otimes|y\rangle\otimes U^{2x}|\psi\rangle$$

$$R_2 \, |x\rangle \otimes |y\rangle \otimes |\psi\rangle = |x\rangle \otimes |y\rangle \otimes U^y |\psi\rangle.$$

Soit maintenant la matrice unitaire

$$S = ((QFT)^\dagger \otimes I_n) \; R_2 \; R_1 \; (H \otimes H \otimes I_n)$$

où H est la matrice de Hadamard usuelle et I_n est la matrice unité agissant sur n qubits. Ici $(QFT)^\dagger$ est l'adjoint de QFT (c.à.d transposé et complexe conjugué).

(a) Quelle est la dimension de la matrice unitaire S ? Faites un dessin du circuit correspondant à S.

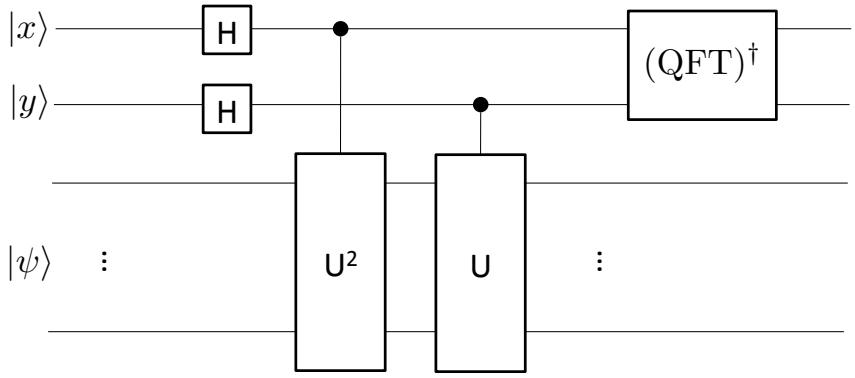
(b) On initialise le circuit dans l'état $|0\rangle \otimes |0\rangle \otimes |u\rangle$. Calculez l'état des $2+n$ qubits juste avant la porte $(QFT)^\dagger$.

(c) Vérifiez que l'expression trouvée sous (b) n'est rien d'autre que $QFT|\varphi_1, \varphi_0\rangle$. Quel est donc l'état à la sortie du circuit ?

(d) En déduire que l'on peut découvrir φ en faisant *une et une seule mesure* des deux premiers qubits à la sortie du circuit.

Solution pour l'exercice 3 :

(a) $\dim(S) = \dim(|x\rangle) \times \dim(|y\rangle) \times \dim(|\psi\rangle) = \dim(\mathbb{C}^2) \times \dim(\mathbb{C}^2) \times \dim\big((\mathbb{C}^2)^{\otimes n}\big) = 2^{2+n}$.
Le circuit correspondant à S :



(b) L'état après les H : $H\,|0\rangle \otimes H\,|0\rangle \otimes |\Psi\rangle = \frac{1}{2}\big(\,|00\psi\rangle + |01\psi\rangle + |10\psi\rangle + |11\psi\rangle\,\big)$
L'état après U^{2x} (ou R_1) : $\frac{1}{2}\big(\,|00\psi\rangle + |01\psi\rangle + e^{4\pi i\varphi}\,|10\psi\rangle + e^{4\pi i\varphi}\,|11\psi\rangle\,\big)$
L'état après U^y (ou R_2) : $\frac{1}{2}\big(\,|00\psi\rangle + e^{2\pi i\varphi}\,|01\psi\rangle + e^{4\pi i\varphi}\,|10\psi\rangle + e^{6\pi i\varphi}\,|11\psi\rangle\,\big)$

(c) On peut écrire la dernière expression comme

$$\frac{1}{2} \sum_{y_1, y_0 \in \{0,1\}} e^{2\pi i \varphi (2y_1 + y_0)} \, |y_1, y_0\rangle \otimes |\psi\rangle = \frac{1}{2} \sum_{y_1, y_0 \in \{0,1\}} e^{\frac{2\pi i}{4}(2\varphi_1 + \varphi_0)(2y_1 + y_0)} \, |y_1, y_0\rangle \otimes |\psi\rangle$$
$$= \mathrm{QFT}\,|\varphi_1, \varphi_0\rangle \otimes |\psi\rangle$$

QFT est unitaire et donc $(QFT)^\dagger(QFT) = I_n$. Alors l'état à la sortie du circuit est $|\varphi_1\rangle \otimes |\varphi_0\rangle \otimes |\psi\rangle$.

(d) Il suffit de mesurer les 2 premiers qubits, parce qu'ils sont $|\varphi_1\rangle \otimes |\varphi_0\rangle$.