Solution de la série 9
Traitement Quantique de l'Information

Exercice 1 *Une autre représentation Porte de Toffoli CCNOT*

1a) On dénote par CU la porte Control-U.

$$1 \otimes CU \left|x, y, z\right\rangle = \left|x\right\rangle \otimes \left|y\right\rangle \otimes U^y \left|z\right\rangle$$

$$(\mathrm{CNOT} \otimes 1)(1 \otimes CU) \left|x, y, z\right\rangle = \left|x\right\rangle \otimes \left|y \oplus x\right\rangle \otimes U^y \left|z\right\rangle$$

$$(1 \otimes CU^\dagger)(\mathrm{CNOT} \otimes 1)(1 \otimes CU) \left|x, y, z\right\rangle = \left|x\right\rangle \otimes \left|y \oplus x\right\rangle \otimes (U^\dagger)^{x \oplus y} U^y \left|z\right\rangle$$

$$(\mathrm{CNOT} \otimes 1)(1 \otimes CU^\dagger)(\mathrm{CNOT} \otimes 1)(1 \otimes CU) \left|x, y, z\right\rangle = \left|x\right\rangle \otimes \left|y\right\rangle \otimes (U^\dagger)^{x \oplus y} U^y \left|z\right\rangle$$

Dernière $CU(\mathrm{CNOT}\otimes 1)(1\otimes CU^\dagger)(\mathrm{CNOT}\otimes 1)(1\otimes CU) \left|x, y, z\right\rangle = \left|x\right\rangle\otimes\left|y\right\rangle\otimes U^x (U^\dagger)^{x\oplus y} U^y \left|z\right\rangle$

Notons que $U^{2xy} = U^x U^{\dagger^{x\oplus y}} U^y = U^{x+y-(x\oplus y)}$ et que $2xy = x + y - (x \oplus y)$. Cela achève la preuve voulue.
On peut aussi vérifier le dernier point plus explicitement en regardant tous les cas. En effet
- si $x = 1, y = 1$ on a $U^2 = U(U^\dagger)^0 U$
- si $x = 1, y = 0$ on a $U^0 = UU^\dagger U^0$
- si $x = 0, y = 1$ on a $U^0 = U^0 U^\dagger U$
- si $x = 0, y = 0$ on a $U^0 = U^0 (U^\dagger)^0 U^0$.

1b) *1ère méthode :*

Pour réaliser un CCNOT il faut prendre $U^2 = \mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Donc $U = \sqrt{\mathrm{NOT}}$. Comemnt calcule-t-on cette matrice ? La meilleure manière est d'utiliser la décomposition spectrale :

$$NOT = (+1)|+\rangle\langle+| + (-1)|-\rangle\langle-|$$

ou $|\pm\rangle$ et ± 1 sont les vecteurs propres et valeurs propres associées. La racine carrée de cette matrice est donnée par (par définition)

$$\sqrt{NOT} = \sqrt{(+1)}|+\rangle\langle+| + \sqrt{(-1)}|-\rangle\langle-|$$

En utilisant que $\sqrt{-1} = i$ et $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ on peut écrire la matrice comme

$$\frac{1+i}{2}|0\rangle\langle 0| + \frac{1-i}{2}|0\rangle\langle 1| + \frac{1+i}{2}|1\rangle\langle 0| + \frac{1+i}{2}|1\rangle\langle 1|$$

En composante on a la représentation

$$\sqrt{\mathrm{NOT}} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1+i}{2} & \frac{1+i}{2} \end{pmatrix}$$

Il est rassurant de vérifier que

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

2ème méthode :

On utilise la décomposition en éléments propres de U, c'est-à-dire $U = PDP^{-1}$. On a alors $U^2 = PDP^{-1}PDP^{-1} = PD^2P^{-1}$. Ici on cherche U qui satisfait $U^2 = X$. A l'aide des valeurs et vecteurs propres de X (cf. série 4) on trouve :

$$U^2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Pour trouver U il suffit de prendre la racine carrée de la matrice diagonale. Ainsi :

$$\begin{aligned} U &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ i & -i \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \end{aligned}$$

Nous arrivons donc bien au même résultat.

Exercice 2 *Un petit algorithme quantique*

2a)

$$H|0\rangle \otimes |u\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |u\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |u\rangle$$

$$CUH|0\rangle \otimes |u\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |u\rangle + \frac{1}{\sqrt{2}}e^{2\pi i\varphi}|1\rangle \otimes |u\rangle$$

$$
\begin{aligned}
HCUH\,|0\rangle \otimes |u\rangle &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes |u\rangle + \frac{e^{2\pi i\varphi}}{2}(|0\rangle - |1\rangle) \otimes |u\rangle \\
&= \frac{1 + e^{2\pi i\varphi}}{2}\,|0\rangle \otimes |u\rangle + \frac{1 - e^{2\pi i\varphi}}{2}\,|1\rangle \otimes |u\rangle \\
&= e^{\pi i\varphi}(\cos \pi\varphi\,|0\rangle \otimes |u\rangle - i \sin \pi\varphi\,|1\rangle \otimes |u\rangle) \\
&= |\psi_{fin}\rangle
\end{aligned}
$$

2b)

$$\text{Prob}(0) = \cos^2 \pi\varphi \;\text{ et }\quad \text{Prob}(1) = \sin^2 \pi\varphi$$

Pour calculer la probabilité d'obtenir l'état $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ on utilise le projecteur $P = \big(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\big)\big(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\big) \otimes \mathbb{I}$. On calcule donc $\langle\psi_{fin}|P|\psi_{fin}\rangle$:

$$
\begin{aligned}
P|\psi_{fin}\rangle &= \left\{\big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\big)\big(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\big) \otimes \mathbb{I}\right\}\left\{e^{\pi i\varphi}(\cos \pi\varphi\,|0\rangle \otimes |u\rangle - i \sin \pi\varphi\,|1\rangle \otimes |u\rangle)\right\} \\
&= e^{\pi i\varphi}\left((\cos \pi\varphi)\frac{|0\rangle + |1\rangle}{2} \otimes |u\rangle - i(\sin \pi\varphi)\frac{|0\rangle + |1\rangle}{2} \otimes |u\rangle)\right)
\end{aligned}
$$

On obtient finalement :

$$
\begin{aligned}
\text{Prob}(\frac{|0\rangle + |1\rangle}{\sqrt{2}}) &= \langle\psi_{fin}|P|\psi_{fin}\rangle \\
&= \frac{1}{2}\cos(\pi\varphi)^2 + \frac{1}{2}\sin(\pi\varphi)^2 \\
&= \frac{1}{2}
\end{aligned}
$$

De manière analogue on trouve $\text{Prob}(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \frac{1}{2}$

Pour calculer la probabilité d'obtenir l'état $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$ on utilise cette fois le projecteur $P = \big(\frac{|0\rangle+i|1\rangle}{\sqrt{2}}\big)\big(\frac{\langle 0|-i\langle 1|}{\sqrt{2}}\big) \otimes \mathbb{I}$. On obtient alors :

$$
\begin{aligned}
P|\psi_{fin}\rangle &= \left\{\big(\frac{|0\rangle + i|1\rangle}{\sqrt{2}}\big)\big(\frac{\langle 0| - i\langle 1|}{\sqrt{2}}\big) \otimes \mathbb{I}\right\}\left\{e^{\pi i\varphi}(\cos \pi\varphi\,|0\rangle \otimes |u\rangle - i \sin \pi\varphi\,|1\rangle \otimes |u\rangle)\right\} \\
&= e^{\pi i\varphi}\left((\cos \pi\varphi)\frac{|0\rangle + i|1\rangle}{2} \otimes |u\rangle - (\sin \pi\varphi)\frac{|0\rangle + i|1\rangle}{2} \otimes |u\rangle)\right)
\end{aligned}
$$

Donc :

$$\begin{aligned}\text{Prob}(\frac{|0\rangle + i|1\rangle}{\sqrt{2}}) &= \langle\psi_{fin}|P|\psi_{fin}\rangle \\ &= \frac{1}{2}\cos(\pi\varphi)^2 + \frac{1}{2}\sin(\pi\varphi)^2 \\ &= \frac{1}{2}\end{aligned}$$

De nouveau en procédant de la même façon on trouve $\text{Prob}(\frac{|0\rangle - i|1\rangle}{\sqrt{2}}) = \frac{1}{2}$

2c) Si on applique U^k au lieu de U on trouve la sortie :

$$e^{i\pi k\varphi}(\cos(\pi k\varphi)\,|0\rangle \otimes |u\rangle - i\sin(\pi k\varphi)\,|1\rangle \otimes |u\rangle)$$

Si $\varphi = \frac{\varphi_1}{2} + \frac{\varphi_2}{2^2} + ... + \frac{\varphi_{t-1}}{2^{t-1}} + \frac{\varphi_t}{2^t}$ en prenant $k = 2^{t-1}$ on observe 0 avec probabilité

$$\text{Prob}(0) = \cos^2(\pi\varphi_{t-1} + \frac{\pi\varphi_t}{2}) = \cos^2(\frac{\pi\varphi_t}{2}) = \begin{cases} 1 & \text{si } \varphi_t = 0 \\ 0 & \text{si } \varphi_t = 1 \end{cases}$$

Exercice 3 *Vérification pour bonne compréhension si besoin est*

(a) Prendre b=0 :

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\sum_{c=0}^{1}|c\rangle.$$

Prendre b=1 :

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\sum_{c=0}^{1}(-1)^c|c\rangle.$$

Pour $m = 2$:

$$\begin{aligned}H^{\otimes 2}|0_2\rangle = (H\otimes H)|00\rangle &= (H\otimes H)|0\rangle \otimes |0\rangle \\ &= H|0\rangle \otimes H|0\rangle \\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle\otimes|0\rangle + |1\rangle\otimes|0\rangle + |0\rangle\otimes|1\rangle + |1\rangle\otimes|1\rangle}{2} \\ &= \frac{1}{(\sqrt{2})^2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle).\end{aligned}$$

De même on vérifie de manière générale que

$$\begin{aligned} H^{\otimes 2}|b_1 b_2\rangle &= H|b_1\rangle \otimes H|b_2\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{c_1} (-1)^{b_1 c_1} |c_1\rangle \otimes \sum_{c_2} (-1)^{b_2 c_2} |c_2\rangle \\ &= (\frac{1}{\sqrt{2}})^2 \sum_{c_1, c_2} (-1)^{b_1 c_1} (-1)^{b_2 c_2} |c_1\rangle \otimes |c_2\rangle \\ &= (\frac{1}{\sqrt{2}})^2 \sum_{c_1, c_2} (-1)^{b_1 c_1 + b_2 c_2} |c_1 c_2\rangle. \end{aligned}$$

Exercice 4 *Variante sur l'algorithme de Deutsch-Josza*

(a) Le vecteur $\underline{a} = (a_1, \cdots, a_n)$ possède n composantes, donc il faut n équations du type $f(\underline{x}) = \underline{a}.\underline{x} + b$ pour le déterminer. Donc il faut n valeurs de $f(\underline{x})$ et il faut poser n questions á l'oracle classique.

(b) En reprenant le circuit quantique de Deutsch-Josza du cours, l' état final de sortie juste avant la mesure est :

$$|\psi_{fin}\rangle = \sum_{c_1, \cdots, c_n} \left\{ \frac{1}{2^n} \sum_{\underline{x}} (-1)^{f(x)} (-1)^{\underline{x}.\underline{c}} \right\} |c_1 \cdots c_n\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

Pour $f(\underline{x}) = \underline{a}.\underline{x} \oplus b$ grâce à l'indication :

$$\begin{aligned} \sum_{\underline{x}} (-1)^{f(x)} (-1)^{\underline{x}.\underline{c}} &= (-1)^b \sum_{\underline{x}} (-1)^{(\underline{a} \oplus \underline{c}).\underline{x}} \\ &= (-1)^b \, 2^n \text{ si } \underline{a} \oplus \underline{c} = 0 \text{ et } = 0 \text{ sinon .} \end{aligned}$$

Ainsi

$$|\psi_{fin}\rangle = (-1)^b \, |c\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

Notons que comme $\underline{a} \oplus \underline{c} = 0$, nous avons $\underline{a} = \underline{c}$ et donc $|c\rangle = |a\rangle$. Ce résultat est remarquable car avec 1 seule mesure des n premiers qubits au trouve $\underline{a}$ avec probabilité 1 !

Preuve de l' indication :

$$\begin{aligned} \sum_{\underline{x} \in \mathbb{F}_2^n} (-1)^{\underline{x}.\underline{z}} &= \sum_{x_1, \cdots, x_n} (-1)^{x_1 z_1} (-1)^{x_2 z_2} \cdots (-1)^{x_n z_n} \\ &= (\sum_{x_1} (-1)^{x_1 z_1}) (\sum_{x_2} (-1)^{x_2 z_2}) \cdots (\sum_{x_n} (-1)^{x_n z_n}) \\ &= (1 + (-1)^{z_1})(1 + (-1)^{z_2}) \cdots (1 + (-1)^{z_n}). \end{aligned}$$

- Si $(z_1, \cdots, z_n) = (0, \cdots, 0)$ on trouve 2^n.

- Sinon au moins un des $z_i \neq 0$ (et donc ce $z_i = 1$) et puisque $1 + (-1)^{z_i} = 1 + (-1) = 0$ on trouve 0 pour le produit ci-dessus.