Solution de la série 4
Traitement quantique de l'information II

Exercice 1 *Porte de Toffoli CCNOT*

1a)

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

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

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

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

Dernière $CU(\text{CNOT}\otimes 1)(1\otimes CU^+)(\text{CNOT}\otimes 1)(1\otimes CU) \, |x, y, z\rangle = |x\rangle \otimes |y\rangle \otimes U^x (U^+)^{x \oplus y} U^y \, |z\rangle$

Notons que $U^{2xy} = U^x U^{+^{x \oplus y}} U^y$. En effet
si $x = 1, y = 1$ on a $U^2 = U(U^+)^0 U$
si $x = 1, y = 0$ on a $U^0 = UU^+U^0$
si $x = 0, y = 1$ on a $U^0 = U^0 U^+ U$
si $x = 0, y = 0$ on a $U^0 = U^0 (U^+)^0 U^0$ cqfd.

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

Donc $U = \sqrt{\text{NOT}}$. On peut verifier que

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

Donc,

$$\sqrt{\text{NOT}} = \frac{1}{\sqrt{2i}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \frac{e^{-i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

Exercice 2 *Un petit algorithme quantique*

2a)

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

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

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

2b)

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

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 *Algorithme de Simon*

Ici le carré est partitionné comme suit :
Soit $X = \{\alpha, \beta\}$. On a $f(00) = f(10) = \alpha$ et $f(01) = f(11) = \beta$.
L'état initial est $|0000\rangle$. Après les premières portes de Hadamard :

$$(\frac{1}{\sqrt{2}})^2\big(|0000\rangle + |0100\rangle + |1000\rangle + |1100\rangle\big).$$

Après l'oracle :

$$(\frac{1}{\sqrt{2}})^2\big(|00\rangle \otimes |f(00)\rangle + |01\rangle \otimes |f(01)\rangle + |10\rangle \otimes |f(10)\rangle + |11\rangle \otimes |f(11)\rangle\big).$$

Ce qui est égal à

$$\begin{aligned} &(\frac{1}{\sqrt{2}})^2\big(|00\rangle|\alpha\rangle + |10\rangle|\alpha\rangle + |01\rangle|\beta\rangle + |11\rangle|\beta\rangle\big) \\ &= (\frac{1}{\sqrt{2}})^2\big((|00\rangle + |10\rangle)|\alpha\rangle + (|01\rangle + |11\rangle)|\beta\rangle\big). \end{aligned}$$

On applique les deux dernières portes de Hadamard :

$$\begin{aligned}
(\frac{1}{\sqrt{2}})^2(\frac{1}{\sqrt{2}})^2 \Big\{ & (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |\alpha\rangle \\
& + (|00\rangle + |01\rangle - |10\rangle - |11\rangle) \otimes |\alpha\rangle \\
& + (|00\rangle - |01\rangle + |10\rangle - |11\rangle) \otimes |\beta\rangle \\
& + (|00\rangle - |01\rangle - |10\rangle + |11\rangle) \otimes |\beta\rangle \Big\}
\end{aligned}$$

$$= \frac{1}{4}\{|00\rangle \otimes (2|\alpha\rangle + 2|\beta\rangle) + |01\rangle \otimes (2|\alpha\rangle - 2|\beta\rangle)\}.$$

Remarquez que les autres termes correspondant à $|10\rangle$ et $|11\rangle$ donnent zéro.
La mesure des deux premiers qubits réduit l'état à $|00\rangle$ ou $|01\rangle$ (pour les deux premiers qubits). Donc on obtient les vecteurs (00) ou (01) $\perp$ à $\vec{a} = (10)$.
Dès que l'on obtient (01) (en répétant l'expérience si besoin est c.à.d au cas où l'on manque de chance on tombe sur (00) ...) on résoud l'équation (condition d'orthogonalité)

$$a_1.0 + a_2.1 = 0,$$

qui possède la solution non triviale unique $a_1 = 1$, $a_2 = 0$.