Solution de la série 10
Traitement Quantique de l'Information

Exercice 1 *Une autre représentation Porte de Toffoli CCNOT*

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

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

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

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

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

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

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 $U^2 = U(U^\dagger)^0U$
- si $x = 1, y = 0$ on a $U^0 = UU^\dagger U^0$
- si $x = 0, y = 1$ on a $U^0 = U^0U^\dagger U$
- si $x = 0, y = 0$ on a $U^0 = U^0(U^\dagger)^0U^0$.

1b) 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

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

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)

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

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

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