G.5 Racine carrée de la porte SWAP

Enoncé : Connaissant le résultat de l'exercice G.3 et celui de l'exercice G.4, écrire la matrice de la racine carrée de la porte SWAP dans $\mathbb{C}^4$

G.5.1 Solution

La description de cette porte est évidente connaissant $\sqrt{CX}$. On a effet vue plus haut que $SWAP = CX \times \overline{CX} \times CX$. On en déduit que $\sqrt{SWAP} = CX \times \sqrt{\overline{CX}} \times CX$, en effet, il est simple de vérifier que

$$\begin{aligned}
\sqrt{SWAP} \times \sqrt{SWAP} &= (CX \times \sqrt{\overline{CX}} \times CX) \times (CX \times \sqrt{\overline{CX}} \times CX) \\
&= CX \times \sqrt{\overline{CX}} \times \sqrt{\overline{CX}} \times CX \\
&= CX \times \overline{CX} \times CX \\
&= SWAP
\end{aligned}$$

De la même manière qu'on a établi la matrice de $\overline{CX}$ il est simple d'établir la matrice de $\sqrt{\overline{CX}}$:

$$\sqrt{\overline{CX}} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix}$$

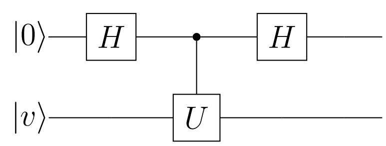
Par conséquent, la matrice de $\sqrt{SWAP}$ va s'écrire de la manière suivante :

$$\begin{aligned}
\sqrt{SWAP} &= CX \times \sqrt{\overline{CX}} \times CX \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 1-i & 0 \\ 0 & 1-i & 1+i & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}
\end{aligned}$$

G.6 Phase kick-back ou rebond de phase

Le phénomène de *phase kick-back* ou "rebond de phase" a déjà été observé dans les algorithmes vus précédemment.

Considérons le circuit quantique suivant :



U est un opérateur unitaire. On lui présente un état $|u\rangle$ qui est l'un de ses vecteurs propres. Comme U est unitaire, ses valeurs propres sont de module 1, donc il existe donc ϕ tel que $U|u\rangle = e^{i\phi}|u\rangle$.

Regardons le déroulement du circuit. Après la porte H sur le fil du haut, on a l'état global tel que

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle|u\rangle)$$

On applique la porte U contrôlée, elle ne fait rien sur le membre de gauche (qui porte $|1\rangle$) mais elle agit sur le membre de droite qui porte $|1\rangle$. On obtient donc :

$$\frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle U|u\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle e^{i\phi}|u\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)|u\rangle$$

Appliquons maintenant une porte de Hadamard sur le qubit du haut. Le second qubit reste à $|u\rangle$, on ne s'y intéresse pas dans le reste de l'équation.

L'action de H sur le premier qubit donne ceci :

$$\begin{aligned}
H(\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)) &= \frac{1}{\sqrt{2}}(H|0\rangle + e^{i\phi}H|1\rangle) \\
&= \frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}e^{i\phi}(|0\rangle - |1\rangle)] \\
&= \frac{1}{2}[(1 + e^{i\phi}|0\rangle + (1 - e^{i\phi})|1\rangle] \\
&= e^{i\phi/2}[\frac{e^{-i\phi/2} + e^{i\phi/2}}{2} - i\frac{e^{-i\phi/2} - e^{i\phi/2}}{2i}] \\
&= e^{i\phi/2}(cos(\phi/2)|0\rangle - i.sin(\phi/2)|1\rangle) \\
&\equiv (cos(\phi/2)|0\rangle - i.sin(\phi/2)|1\rangle)
\end{aligned}$$

A un terme de phase (non mesurable) près, l'état du premier qubit est $cos(\phi/2)|0\rangle - i.sin(\phi/2)|1\rangle$. On observe un effet de phase du au fait que $|u\rangle$ était un vecteur propre de U.

La chose la plus intéressante a observé est de voir que, bien que U agisse sur le second qubit, c'est le premier qui subit cet effet de phase.

G.7 Démonstration du théorème de non-clonage

Il est légitime de se demander s'il est possible de dupliquer un état quantique, en d'autres termes existe-t'il un opérateur unitaire U tel que $U(|x\rangle|0\rangle \to |x\rangle|x\rangle$.

On peut être tenté de se dire que la porte CNOT permet de faire une telle opération. En effet, si l'on considère les seuls états de base $|0\rangle$ et $|1\rangle$, l'effet de la porte CNOT est $|x\rangle|y\rangle \to |x\rangle|x \oplus y\rangle$, et donc $|x\rangle|0\rangle \to |x\rangle|x\rangle$.

Il est toutefois simple de vérifier que cette constatation n'est pas généralisable à tous les états, en effet si l'on considère un état générique $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, quel est l'effet de la porte CNOT sur $|\phi\rangle \otimes |0\rangle$? Si l'on déroule un peu les calculs d'algèbre, on trouve que

$$|\phi\rangle \otimes |0\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle$$

La porte CNOT laisse $|00\rangle$ inchangé mais transforme $|10\rangle$ en $|11\rangle$, la porte CNOT change donc $|\phi\rangle$ en $\alpha|00\rangle + \beta|11\rangle$ qui est un état intriqué (non factorisable) très différent de $|\phi\rangle \otimes |\phi\rangle$ (factorisé par construction). CNOT ne duplique pas les états.

D'une manière générale, on peut prouver qu'il est impossible de cloner les états quantiques. En voici la démonstration.

Démonstration avec seulement 2 qubits

Supposons qu'il existe un opérateur U unitaire tel que $U|x\rangle|0\rangle = |x\rangle|x\rangle$. Par conséquent,

$$U|00\rangle = |00\rangle \text{ et } U|10\rangle = |11\rangle$$

Par conséquent

$$U(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = U(\frac{|00\rangle}{\sqrt{2}}) + U(\frac{|10\rangle}{\sqrt{2}}) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Cependant, on remarque que $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = (\frac{|0\rangle+|1\rangle}{\sqrt{2}})|0\rangle$

On devrait donc avoir

$$\begin{aligned} U(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) &= U((\frac{|0\rangle + |1\rangle}{\sqrt{2}})|0\rangle) \\ &= (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \end{aligned}$$

On a donc un état dont l'image par U est à la fois un état intriqué $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et un état non intriqué (car factorisé) $(\frac{|0\rangle+|1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle+|1\rangle}{\sqrt{2}})$ ce qui est une évidente contradiction.

Démonstration avec n qubits

Le cas général à n qubits se démontre d'une manière similaire au "cas simple" avec deux qubits. Soit n qubit, on peut écrire les n vecteurs de la base canonique sous la forme $|0\rangle, |1\rangle, |2\rangle, \cdots |2^n - 1\rangle$.

Supposons qu'il existe un opérateur A tel que $\forall |\phi\rangle, A|\phi\rangle|0^{\otimes n}\rangle = |\phi\rangle|\phi\rangle$

On va s'intéresser aux états $|\phi_0\rangle = |00\cdots 00\rangle$ et $|\phi_1\rangle = |00\cdots 01\rangle$

$$\begin{aligned} A|\phi_0\rangle|0^{\otimes n}\rangle &= |\phi_0\rangle|\phi_0\rangle \\ A|\phi_1\rangle|0^{\otimes n}\rangle &= |\phi_1\rangle|\phi_1\rangle \end{aligned}$$