Traitement quantique de l'information I (automne 2009)
Corrigé 10

1. Le CNOT prend comme input $|x, y\rangle$ et rend comme output $|x, y \oplus x\rangle$, où $\oplus$ est la somme module 2. On remarque tout d'abord que $y \oplus (y \oplus x) = x$. Quels peuvent être les états en entrée d'un CNOT, pour obtenir à la sortie $|y, x\rangle$? Si en entrée nous avions $|y, y \oplus x\rangle$, alors on aurait

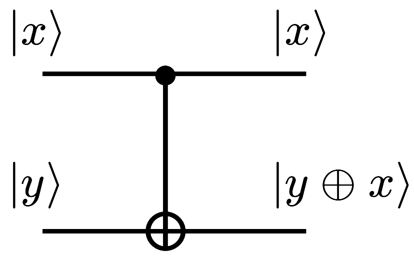
$$U_{\text{CNOT}}|y, y \oplus x\rangle = |y, y \oplus (y \oplus x)\rangle = |y, x\rangle$$

Nous devrions maintenant obtenir $|y, y \oplus x\rangle$ d'une opération CNOT. L'idée est de partir de l'état $|x, y \oplus x\rangle$ et appliquer un CNOT **avec les deux entrées inversées**. Dans ce cas nous aurions

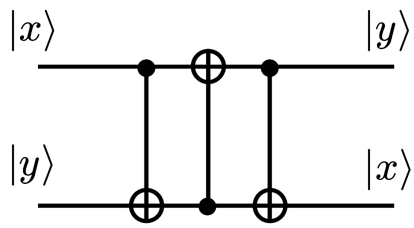
$$U'_{\text{CNOT}}|x, y \oplus x\rangle = |x \oplus (y \oplus x), y \oplus x\rangle = |y, y \oplus x\rangle$$

Pour finir, on remqrque que l'état $|x, y \oplus x\rangle$ est la sortie d'un CNOT avec en entrée $|x, y\rangle$.

Donc il faut appliquer trois CNOT, dont celui du milieu est inversé. Si on indique le CNOT par le symbole suivant alors l'opération de SWAP



est donnée par la porte logique suivante



2. Avec un CNOT on peut copier les états $|0\rangle$ et $|1\rangle$. Il suffit que l'état soit appliqué à l'entrée de controle et que $|0\rangle$ soit appliqué à l'entrée principale.

   $$U_{\text{CNOT}}|x, 0\rangle = |x, x\rangle$$

   Donc on sait copier $|0\rangle \to |00\rangle$ et $|1\rangle \to |11\rangle$.

   Considérons maintenant l'état

   $$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

   L'entrée du CNOT sera maintenant

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

   Par linéarité, à la sortie on aura

   $$U_{\text{CNOT}}|\phi\rangle = \alpha|00\rangle + \beta|11\rangle$$

   Cet état est un état intriqué et ne correspond pas à l'état non intriqué $|\psi\rangle \otimes |\psi\rangle$ qu'il aurait fallu obtenir pour copier avec succes l'état $|\psi\rangle$.

   De manière plus générale, l'impossibilité de copier un état quantique arbitraire est assurée par le *no-cloning theorem*.