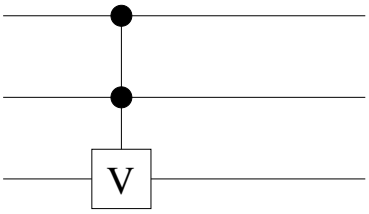
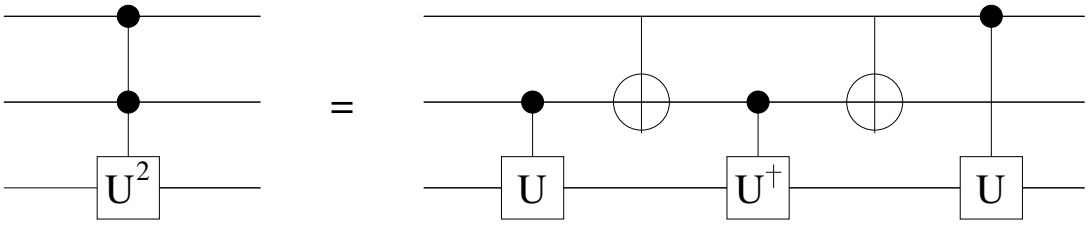
Série 9
Traitement Quantique de l'Information

Exercice 1 *Encore une représentation de la porte de Toffoli CCNOT*

Soit V une matrice 2×2 unitaire.
La porte "double contrôle-V" notée CCV est définie par le circuit suivant :



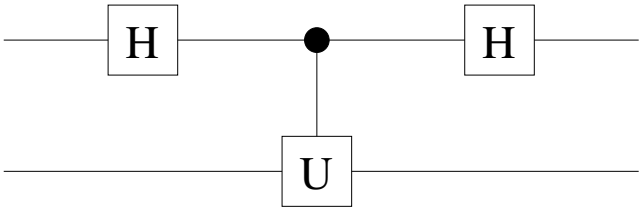
1a) Montrez que pour tout U unitaire 2×2 :



1b) Comment choisir U pour réaliser la porte de Toffoli CCNOT ? Donnez explicitement une telle matrice U.

Exercice 2 *Un petit algorithme quantique*

Soit U une matrice unitaire et $|u\rangle$ un vecteur propre, c'est à dire $U|u\rangle = \exp(2\pi i\varphi)|u\rangle$. Considérez le circuit suivant :



3a) Calculez la sortie pour l'état initial $|0\rangle \otimes |u\rangle$.

3b) Calculez la probabilité d'observer le premier bit dans l'état $|0\rangle$ à la sortie. Même question pour la probabilité d'observer le premier bit dans l'état $|1\rangle$ à la sortie.

Question facultative : Même question pour les probabilités d'observer $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$; $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$; $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$ et $\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$ à la sortie.

3c) Supposons que l'on remplace U par U^k, k entier dans le circuit ci-dessus. Soit $\varphi = 0, \varphi_1\varphi_2...\varphi_t$ le développement binaire de $0 < \varphi < 1$. Comment choisir k pour déterminer le bit le moins significatif φ_t en une seule mesure ?

Exercice 3 *Facultatif : vérification pour bonne compréhension si besoin est. Sinon passez directement au prochain exercice.*

On adopte la notation $|b\rangle$, $|c\rangle$ pour les états de la base canonique $|1\rangle$, $|0\rangle$ (c.à.d. que $b = 0, 1$ et $c = 0, 1$). Vérifiez que

$$\begin{aligned} H|b\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\sum_{c=0}^{1}(-1)^{bc}|c\rangle \end{aligned}$$

et vérifiez pour $n = 2$

$$H^{\otimes n}|b_1, ..., b_n\rangle = \frac{1}{\sqrt{2^n}}\sum_{(c_1,...,c_n)\in\mathbb{F}_2^n}(-1)^{\sum_{i=1}^n b_i c_i}|c_1, ..., c_n\rangle$$

et ensuite le cas général.

Exercice 4 *Variation sur le problème de Deutsch-Josza*

En 1993 E. Bernstein et U. Vazirani (Proc, 25th Annual ACM Symposium on the Theory of Computing, ACM Press, NY p11-20) formulèrent le problème suivant. On se donne un "oracle" qui calcule

$$f(\underline{x}) = \underline{a}\cdot\underline{x} \oplus b \mod 2$$

pour chaque entrée $\underline{x} \in \mathbb{F}_2^n$. Ici $\underline{a} \in \mathbb{F}_2^n$ et $b \in \mathbb{F}_2$. Le but est de calculer $\underline{a}$ en posant le moins de questions possibles à l'oracle.

1. Combien de questions faut-il poser à l'oracle pour déterminer $\underline{a}$ classiquement ?
2. Montrez que
$$\sum_{\underline{x}\in\mathbb{F}_2^n}(-1)^{\underline{x}\cdot\underline{z}} = \begin{cases} 2^n & \text{si } \underline{z} = (0, 0, ..., 0) \\ 0 & \text{sinon} \end{cases}$$
3. En utilisant le point précédent montrez que grâce au circuit de Deutsch-Josza, il suffit de poser une seule question à "l'oracle quantique" pour déterminer $\underline{a}$.