Série 6
Traitement quantique de l'information II

Exercice 1 *Période d'une fonction et factorisation de $N = 15$*

On veut factoriser le nombre $N = 15$ grâce à l'algorithme aléatoire vu en cours. Pour cela on tire un nombre a au hasard dans $\{2, 3, ..., 15\}$. Nous supposerons que nous avons tiré $a = 7$ qui est premier avec 15.

a) Calculez l'ordre $\mathrm{Ord}\,(7)$ c.à.d. le plus petit entier r tel que $7^r = 1 \bmod 15$. Pour cela vous calculerez les premières valeurs de la fonction $f : x \to f(x) = 7^x \bmod 15$.

b) Expliciter les étapes ultérieures de l'algorithme classique.

c) On veut maintenant expliciter l'algorithme quantique pour la recherche de l'ordre. Prendre le circuit quantique pour la période de la fraction $f : x \to (7^x \bmod 15)$ avec $M = 2^{11} = 2048$.

- **c1)** Donnez l'état juste après les portes de Hadamard.
- **c2)** Donnez l'état juste après le circuit de U_f.
- **c3)** Donnez l'état après la QFT.
- **c4)** Montrez que $\mathrm{Pr}\,(y)$ vaut $\frac{1}{4}$ si $y = 0$, 512, 1024 et 1536 et vaut 0 sinon.
- **c5)** Supposons que la mesure nous donne le nombre $y = 1536$. Peut-on trouver r?
- **c6)** Même question si la mesure donne $y = 0$, 512, et 1024 (discuter tous les cas !)

Indications générales : on pourra reprendre les formules générales du cours.

Exercice 2 *Identités utiles pour la réalisation exérimentale de la porte CNOT par RMN*

Dans cet exercice nous prouvons quelques identités utiles à la réalisation expérimentale de la porte CNOT. Elles formeront la base de la discussion du cours, concernant la réalisation expérimentale par RMN des algorithmes de Deutsch-Josza et de Shor (pour 7 à 10 qubits).

On considère deux qubits (par ex. spins 1/2, systèmes à deux niveaux) et les opérateurs suivants :

- Rotations d'angle $-\pi/2$ autour de l'axe z pour un spin :

$$R = \exp\left(i\frac{\pi}{2}\frac{\sigma_z}{2}\right)$$

- Porte de Hadamard H

$$H = \frac{1}{\sqrt{2}}\left(\sigma_z + \sigma_x\right)$$

- L'opérateur d'évolution

$$U = \exp\left(-i\frac{t}{\hbar}\mathcal{H}\right)$$

associé à l'Hamiltonien d'interaction pour deux spins $\mathcal{H} = \hbar J\ \sigma_z \otimes \sigma_z$. On laisse évoluer le système pendant un temps $t = \pi/4J$.

a Ecrire la décomposition spectrale de $\mathcal{H}$ et U.

b Dessinez le circuit correspondant au produit des matrices

$$(\mathbb{I}_{2\times2} \otimes H)\, U\, (R \otimes R)\, (\mathbb{I}_{2\times2} \otimes H)$$

c Calculez ce produit et montrez qu'il est égal à la porte CNOT. On procèdera ainsi : Faire agir le produit sur $|x\rangle \otimes |y\rangle$ et montrez que le résultat est le même que CNOT $|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus x\rangle$.

Exercice 3 *Remarques sur la transformée de Fourier Quantique*

a) Montrer que pour $M = 2$ la transformation QFT n'est rien d'autre qu'une porte de Hadamard H.

b) Ecrire explicitement QFT $|x\rangle$ pour $M = 4$ et $x = 0, 1, 2, 3$.

c) Montrer dans le cas général que QFT est une matrice unitaire. Indication : montrer que

$$\langle x'|\, (\mathrm{QFT})^\dagger\, \mathrm{QFT}\, |x\rangle = \langle x'|x\rangle$$