Série 9
Calcul Quantique

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 $\Pr\,(y)$ 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 *Unitarité de la transformée de Fourier Quantique*

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

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