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.

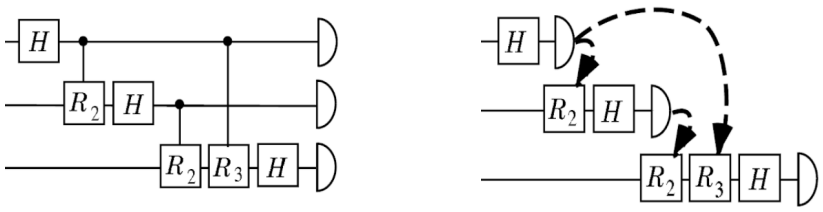
Exercice 2 *Optimization du circuit de l'algorithme de Shor*

Nous avons vu en cours que pour avoir la probabilité de succès dans l'algorithme de Shor assez grande il faut prendre $M\tilde{N}^2$. Nous supposons ici qu'il est possible de répéter l'expérience un nombre de fois aussi grand que voulu. Dans ce cas la période peut etre lue sur l'histogramme des mesures successives.

a) Supposons donc que nous voulions factoriser $N = 15$ sans restriction sur le nombre de mesures faites. Comment choisir de facon optimale la taille du circuit sans supposer les facteurs premiers connus ?

b) Supposons que comme avant $a = 7$ et qu'en plus la période $r = 4$ soit connue (en pratique bien sur si la période est connue l'algorithme perd tout son interet). Optimisez la taille du second registre et dessinez le circuit.

c) Supposons que $a = 11$. Vérifiez qu'alors la période est $a = 2$. A nouveau supposant cette période connue optimisez la taille du second registre.



Exercice 3 *Transformée de Fourier "semi-classique"*

La figure de gauche représente la QFT traditionnelle ou les qbits sont mesurés à la fin du circuit. Dans celle de droite les qbits sont mesués juste après les portes de Hadamard et le résultat de la mesure (qui est un signal classique !) est utilisé pour controller les phase-gates qui suivent.

a) Considérez une entrée qui est un état produit sur les trois qbits et montrez que les deux circuits produisent des histogrammes de mesures identiques.

b) Expliquez en quelques mots comment (en théorie) on pourrait implémenter le circuit de droite avec à notre disposition un "seul bit quantique" comme resource. Ce circuit s'appelle la QFT semi-classique. L' idée à été introduite par Griffiths et Niu en 1996.

c) Expliquez en quelques mots comment (en théorie) implémenter l'algorithme de Shor en utilisant un seul bit quantique dans le premier registre grâce à la QFT semi-classique.