# TD 2 - Algorithme de Grover et algorithme de Shor

Informatique quantique pour la recherche opérationnelle, S5.

2023

**Exercice 1 — *Changeons deux-trois trucs*** Dans cette exercice, on dispose d'une fonction $f$ telle qu'il existe un unique $s \leq 2^n$ tel que $f(s) = 1$. On veut comprendre ce qu'il se passe si on modifie un peu l'entrée de l'algorithme de Grover.

1. Que se passe-t-il si, au lieu de donner $|\underline{0}\rangle$ on donne $-|\underline{0}\rangle$ au circuit de l'algorithme de Grover? S'approche-t-il de la solution ? Si oui, en combien d'itérations ? Si non, comment corriger l'algorithme ?

▶ **Correction**

L'algorithme converge.

Le vecteur $-|\underline{0}\rangle$ passe dans la porte $H^{\otimes n}$. On obtient alors $-\frac{1}{\sqrt{2}}\sum_{x=0}^{2^n-1}|\underline{x}\rangle$.

Ce vecteur est dans le plan généré par $|\underline{s}\rangle$ et $\sum_{x\neq s}|\underline{x}\rangle$. Comme pour la version classique de l'algorithme de Grover, ce vecteur va effectuer une rotation d'angle $\theta$ (où cet angle est le même que dans le cours : $\frac{2}{\sqrt{2}}$).

Pour se rapprocher de $|\underline{s}\rangle$, cet angle doit tourner sur un angle de $\pi + \alpha$ (où $\alpha$ est l'angle qui sépare $H^{\otimes n}|\underline{0}\rangle$ et $|\underline{s}\rangle$, soit $\frac{\pi-\theta}{2}$).

Donc, on doit tourner $\lfloor\frac{3\pi-\theta}{2\theta}\rfloor$ fois, soit environ $\frac{3\pi}{4}\sqrt{n} - \frac{1}{2}$ fois.

2. On suppose que $s > 1$. Mêmes questions si on démarre de $H^{\otimes n}(|\underline{0}\rangle - |\underline{1}\rangle)$.

▶ **Correction**

Si on démarre de ce vecteur alors, après passage dans la porte $H^{\otimes n}$, on obtient $|\underline{0}\rangle - |\underline{1}\rangle$, soit un vecteur orthogonal à $|\underline{s}\rangle$ et $\sum_{x\neq s}|\underline{x}\rangle$. Ce vecteur est donc orthogonal au plan généré par ces deux vecteurs.

Lorsqu'on effectue la porte $O_f$, le vecteur n'est pas changé. Puis, lorsqu'on effectue la symétrie $S$ par rapport à $\sum_x|\underline{x}\rangle$, le vecteur est inversé. Toutes les deux itérations, le vecteur revient à sa position de départ. L'algorithme ne converge donc pas.

On peut corriger le tir, il faudrait envoyer $H^{\otimes n}(|\underline{0}\rangle - |\underline{1}\rangle)$ sur $|\underline{0}\rangle$ avant l'algorithme. Il suffit de mettre une porte $H^{\otimes n}$ suivit d'une porte $H$ sur le premier qbit.

On pourrait aussi se placer dans le plan généré par $|\underline{s}\rangle$ et $|\underline{0}\rangle - |\underline{1}\rangle$. Mais ce n'est pas évident si on ne connait pas $s$.

**Exercice 2 — *Amplification quantique***

Soit une fonction $f : \{0,1\}^n \to \{0,1\}$ telle qu'il existe un unique $s$ tel que $f(s) = 1$. Soient $\varepsilon > 0$ et un algorithme probabiliste $A$ qui, avec une probabilité supérieure à $\varepsilon$, renvoie $s$. On cherche à construire un algorithme $B$ qui renvoie $s$ avec une probabilité supérieure à $\frac{2}{3}$.

**Partie 1. Amplification**

1. (a) Soit $k \in \mathbb{N}$ et $B$ l'algorithme qui appelle $k$ fois l'algorithme $A$. Il renvoie $s$ si au moins une des occurences de $A$ a renvoyé $s$. Quelle est la probabilité que $B$ renvoie $s$ ?

▶ **Correction**

$A$ a une probabilité inférieure à $1-\varepsilon$ de ne pas renvoyer $s$. Donc $B$ a une probabilité inférieure à $(1-\varepsilon)^k$ de ne pas renvoyer $s$. Celle de renvoyer $s$ est donc au moins $1-(1-\varepsilon)^k$.

(b) En déduire la valeur de $k$ nécessaire pour que cette probabilité dépasse $\frac{2}{3}$.

▶ **Correction**

Il faut que

$$\begin{aligned}
1-(1-\varepsilon)^k &\geq \frac{2}{3} \\
\frac{1}{3} &\geq (1-\varepsilon)^k \\
\frac{\ln(\frac{1}{3})}{\ln(1-\varepsilon)} &\leq k \\
\frac{\ln(\frac{1}{3})}{\ln(1-\varepsilon)} &\leq k \\
\frac{\ln(\frac{1}{3})}{-\sum_{i=1}^{+\infty} \varepsilon^i/i} &\leq k \\
\frac{\ln(3)}{\sum_{i=1}^{+\infty} \varepsilon^i/i} &\leq k \\
\frac{\ln(3)}{\varepsilon} &\leq k
\end{aligned}$$

2. On dipose maintenant d'un circuit quantique $QA$ de $A$. Cet algorithme a la propriété suivante: $QA\,|\underline{0}\rangle$ renvoie $\sum_{x=0}^{2^n-1} a_x\,|\underline{x}\rangle$. On suppose $a_x \in \mathbb{R}^+$. Enfin, on suppose $|a_s|^2 \geq \varepsilon$. On suppose $a_s$ et $\varepsilon$ petits.

(a) Quelle est la probabilité qu'on mesure $s$ à l'issue de ce circuit?

▶ **Correction**

La probabilité est $|a_s|^2 \geq \varepsilon$.

(b) Quel est l'angle entre le vecteur $QA\,|\underline{0}\rangle$ et $\sum_{x\neq s} a_x\,|x\rangle$ ?

▶ **Correction**

Le sinus de cet angle est le produit scalaire de $QA\,|\underline{0}\rangle$ et de $|\underline{s}\rangle$ divisé par les normes des deux vecteurs, ici 1. Puisque $QA\,|\underline{0}\rangle = \sum_{x=0}^{2^n-1} a_x\,|\underline{x}\rangle$, on obtient donc $a_s \geq \sqrt{\varepsilon}$.

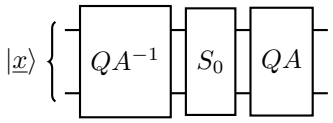
Si on suppose l'angle petit puisque $a_s$ est petit, donc l'angle vaut environ $a_s$.

(c) Quel est l'angle entre le vecteur $QA\,|\underline{0}\rangle$ et $|s\rangle$ ?

▶ **Correction**

On obtient $\pi/2$ moins l'angle précédent, soit $\frac{\pi}{2} - a_s \leq \frac{\pi}{2} - \sqrt{\varepsilon}$.

(d) Que fait le circuit suivant où $S_0$ est la symétrie par rapport à $|\underline{0}\rangle$?



▶ **Correction**

Le circuit effectue une symétrie par rapport à $QA\,|\underline{0}\rangle$.

(e) Proposez un circuit qui permet de mesurer l'état cible avec une probabilité au moins $\frac{2}{3}$. Combien de fois l'algorithme $QA$ est appelé par ce circuit ?

▶ **Correction**

Le circuit construit $QA\,|\underline{0}\rangle$, puis appelle un certain nombre de fois la porte $O_f$ suivie du circuit précédent. A chaque fois, $QA$ est appelée deux fois.

La porte $O_f$ va effectuer une symétrie par rapport $\sum_{x\neq s} a_x\,|\underline{x}\rangle$ et la porte $S$ par rapport $QA\,|0\rangle$. Ces deux symétries effectuent une rotation d'angle au moins $2\sqrt{\varepsilon}$ dans le plan généré par $|s\rangle$ et $\sum_{x\neq s} a_x\,|\underline{x}\rangle$.

Le nombre d'itérations pour atteindre $\frac{2}{3}$ consiste à atteindre un angle de $\pi/3$. Il faut donc au moins
$(\frac{\pi}{3} - \sqrt{\varepsilon})/2\sqrt{\varepsilon}$ itérations, soit environ $\frac{\pi}{6\sqrt{\varepsilon}}$.

**Partie 2. Collision**

On supposera que l'amplification précédente fonctionne également si $s$ n'est pas unique.

On dispose d'une fonction $H : 0,1^n \to 0,1^n$. On cherche $x$ et $y$ tels que $H(x) = H(y)$ et $x \neq y$ (on dit qu'il y a collision). On suppose que, pour tout $x$, il existe une collision avec au moins un autre $y$.

On fixe un entier $k$. On applique l'algorithme suivant:

- Evaluer et trier $H(x)$ pour $x < k$.
- Vérifier s'il y a collision.
- Sinon, choisir $y$ entre $k$ et $2^n - 1$ et répondre OUI si $H(y) = H(x)$ pour $x \leq k$.

1. Quelle est la probabilité de succès de cet algorithme?

▶ **Correction**

Il est de l'ordre de $\frac{k}{2^n-k} \geq \frac{k}{2^n}$ si la collision n'apparait pas dans les $k$ premières valeurs (et 1 si c'est le cas).

2. Proposez un algorithme quantique qui trouve une collision avec une forte probabilité en $O(\sqrt[3]{2^n})$ appels à $H$.

▶ **Correction**

Posons $\varepsilon = \frac{k}{2^n}$.

Avec l'algorithme précédent, on peut amplifier cette probabilité jusqu'à $\frac{2}{3}$ en $O(\frac{1}{\sqrt{\varepsilon}})$ itérations de Grover.

On a donc un algorithme en $O(k + \sqrt{2^n/k})$ appels à $H$. Choisissons maintenant $k = \sqrt[3]{2^n}$, alors cet algorithme effectue $O(\sqrt[3]{2^n} + \sqrt{2^n/\sqrt[3]{2^n}}) = O(\sqrt[3]{2^n} + \sqrt{\sqrt[3]{2^n}^2/2^n}) = O(\sqrt[3]{2^n} + \sqrt[3]{2^n}\sqrt{1/2^n}) = O(\sqrt[3]{2^n})$.

**Exercice 3 — *Exemple d'exécution de l'algorithme de Shor***

Quelles sont les exécutions possibles de l'algorithme de Shor quand on cherche à factoriser 91 ?

▶ **Correction**

Notez que la plupart des calculs ne peuvent se faire à la main. Mais les poser sur le papier permet de mieux comprendre et retenir le fonctionnement de l'algorithme. Vous êtes invités à faire de même avec une autre exécution aléatoire de l'algo.

On cherche à factoriser $n = 91$. On cherche donc $p$ et $q$ deux diviseurs premiers de 91, ici il s'agit de $p = 7$ et $q = 13$.

- On commence par chercher un entier $a$ au hasard entre 1 et $n - 1$. Disons qu'on trouve $a = 23$. On vérifie si $a$ est premier avec $n$. S'il n'est pas premier, leur PGCD donnera $p$ ou $q$. Le nombre 23 est bien premier avec 91 car 23 est premier et qu'il n'est pas un diviseur de 91.

- On va utiliser un algorithme quantique pour calculer l'ordre $r$ de $a$ c'est à dire le plus petit entier $r$ tel que $a^r \equiv 1 \mod n$. Vu que $n$ est petit, on peut le faire par énumération totale ici:

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $a^i$ | 23 | 529 | 12167 | 279841 | 6436343 | 148035889 |
| $a^i \mod n$ | 23 | 74 | 64 | 16 | 4 | 1 |

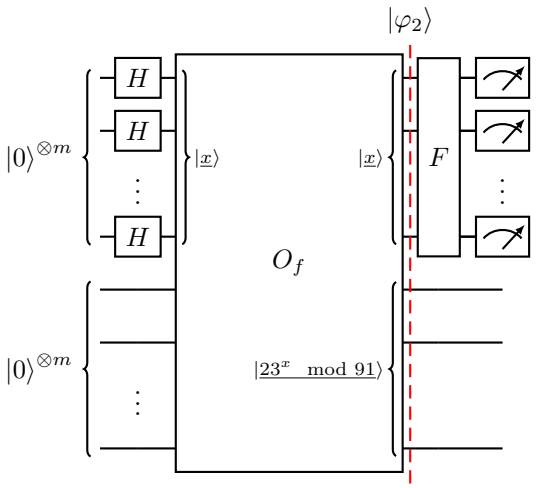
  On devrait donc trouver $r = 6$.

- Puisque l'ordre est pair, on vérifie si $a^{r/2} + 1 \not\equiv 0 \mod n$ ; soit $a^3 + 1 = 12168 \equiv 65 \mod n \not\equiv 0 \mod n$. D'après le cours, le pgcd de $n$ avec $a^{r/2} + 1$ ou $a^{r/2} - 1$ donne 7 et 13.

  C'est bien le cas ici, $PGCD(91, 12168) = 13$ et $PGCD(91, 12166) = 7$.

- Il reste donc pour l'algorithme à trouver $r$ sans méthode brute force.

  On exécute le circuit quantique suivant avec $m$ vérifiant $2^m > n^2$.




  Puisque $91^2 = 8281$, alors on peut prendre $m = 14$ car $2^{14} = 16384$. On a donc un circuit avec 28 qbits.

  Lorsqu'on passe l'entrée dans les portes $H$ et la porte $O_f$, on obtient

$$|\varphi_2\rangle = \frac{1}{\sqrt{16384}} \sum_{x=0}^{16383} |\underline{x}\rangle \otimes |\underline{23^x \mod 91}\rangle$$

Puisque $23^6 \equiv 1 \mod 91$ alors on a 6 valeurs possibles pour $23^x \mod 91$ qui sont les 6 valeurs du tableau donné plus haut: $23, 74, 64, 16, 4$ et $1$.

$$
\begin{aligned}
|\varphi_2\rangle = \frac{1}{\sqrt{16384}}( & \\
& |\underline{0}\rangle \otimes |\underline{1}\rangle + \\
& |\underline{1}\rangle \otimes |\underline{23}\rangle + \\
& |\underline{2}\rangle \otimes |\underline{74}\rangle + \\
& |\underline{3}\rangle \otimes |\underline{64}\rangle + \\
& |\underline{4}\rangle \otimes |\underline{16}\rangle + \\
& |\underline{5}\rangle \otimes |\underline{4}\rangle + \\
& |\underline{6}\rangle \otimes |\underline{1}\rangle + \\
& |\underline{7}\rangle \otimes |\underline{23}\rangle + \\
& |\underline{8}\rangle \otimes |\underline{74}\rangle + \\
& |\underline{9}\rangle \otimes |\underline{64}\rangle + \\
& |\underline{10}\rangle \otimes |\underline{16}\rangle + \\
& |\underline{11}\rangle \otimes |\underline{4}\rangle + \\
& \cdots + \\
& |\underline{16374}\rangle \otimes |\underline{1}\rangle + \\
& |\underline{16375}\rangle \otimes |\underline{23}\rangle + \\
& |\underline{16376}\rangle \otimes |\underline{74}\rangle + \\
& |\underline{16377}\rangle \otimes |\underline{64}\rangle + \\
& |\underline{16378}\rangle \otimes |\underline{16}\rangle + \\
& |\underline{16379}\rangle \otimes |\underline{4}\rangle + \\
& |\underline{16380}\rangle \otimes |\underline{1}\rangle + \\
& |\underline{16381}\rangle \otimes |\underline{23}\rangle + \\
& |\underline{16382}\rangle \otimes |\underline{74}\rangle + \\
& |\underline{16383}\rangle \otimes |\underline{64}\rangle) \\
= \frac{1}{\sqrt{16384}}( & \\
(|\underline{0}\rangle + |\underline{6}\rangle + \cdots |\underline{16374}\rangle + |\underline{16380}\rangle) & \otimes |\underline{1}\rangle + \\
(|\underline{1}\rangle + |\underline{7}\rangle + \cdots |\underline{16375}\rangle + |\underline{16381}\rangle) & \otimes |\underline{23}\rangle + \\
(|\underline{2}\rangle + |\underline{8}\rangle + \cdots |\underline{16376}\rangle + |\underline{16382}\rangle) & \otimes |\underline{74}\rangle + \\
(|\underline{3}\rangle + |\underline{9}\rangle + \cdots |\underline{16377}\rangle + |\underline{16383}\rangle) & \otimes |\underline{64}\rangle + \\
(|\underline{4}\rangle + |\underline{10}\rangle + \cdots |\underline{16378}\rangle) & \otimes |\underline{16}\rangle + \\
(|\underline{5}\rangle + |\underline{11}\rangle + \cdots |\underline{16379}\rangle) & \otimes |\underline{4}\rangle)
\end{aligned}
$$

On retrouve la forme

$$|\varphi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{y=0}^{r-1} \sum_{\substack{x=0 \\ x-y=kr}}^{2^m-1} |\underline{x}\rangle \otimes |\underline{a^y \mod n}\rangle$$

On note qu'il y a 6 groupes de qbits et que 4 d'entres eux possèdent un élément de plus dans la parenthèse. Cela s'explique car $r = 6$ ne divise pas $2^m = 16384$. On a donc 16384 éléments répartis dans 6 groupes, ces groups ne sont nécessairement pas de la même taille.

Dans les 4 premiers groupes (associés à $|\underline{1}\rangle, |\underline{23}\rangle, |\underline{74}\rangle$ et $|\underline{64}\rangle$) il y a $\left\lceil \frac{16384}{6} \right\rceil = 2731$ éléments.

Dans les 2 autres groupes (associés à $|\underline{16}\rangle$ et $|\underline{4}\rangle$) il y a $\lfloor \frac{16384}{6} \rfloor = 2730$ éléments. Cette distinction n'apparait pas si $r$ divise $2^m$.

- On fait une mesure partielle du 2e $m$-qbit. On peut trouver toutes les valeurs possibles de ce qbits: $1, 23, 74, 64, 16$ et $4$. Disons qu'on trouve 74. Notre premier $m$-qbit, intriqué avec le second, devient alors

$$\begin{aligned}|\varphi_3\rangle &= \frac{1}{\sqrt{2731}}( \\ &\quad |\underline{2}\rangle \otimes |\underline{74}\rangle + \\ &\quad |\underline{8}\rangle \otimes |\underline{74}\rangle + \\ &\quad \cdots + \\ &\quad |\underline{16376}\rangle \otimes |\underline{74}\rangle + \\ &\quad |\underline{16382}\rangle \otimes |\underline{74}\rangle) \\ &= \frac{1}{\sqrt{2731}} (|\underline{2}\rangle + |\underline{8}\rangle + \cdots |\underline{16376}\rangle + |\underline{16382}\rangle) \otimes |\underline{74}\rangle\end{aligned}$$

  Si on avait mesuré 4, on aurait eu à la place

$$\begin{aligned}|\varphi_3\rangle &= \frac{1}{\sqrt{2730}}( \\ &\quad |\underline{5}\rangle \otimes |\underline{4}\rangle + \\ &\quad |\underline{11}\rangle \otimes |\underline{4}\rangle + \\ &\quad \cdots + \\ &\quad |\underline{2730}\rangle \otimes |\underline{4}\rangle) \\ &= \frac{1}{\sqrt{2730}} (|\underline{5}\rangle + |\underline{11}\rangle + \cdots |\underline{16379}\rangle) \otimes |\underline{4}\rangle)\end{aligned}$$

  Notez la normalisation du qbit qui change la constante devant le qbit. Reconsidérons donc qu'on a mesuré 74 et non 4.

- On passe le qbit dans la porte $F \otimes Id$. Pour rappel $F|\underline{x}\rangle = \frac{1}{\sqrt{2^m}} \sum_{z=0}^{2^m-1} \omega^{xz} |\underline{z}\rangle = \frac{1}{\sqrt{16384}} \sum_{z=0}^{16383} e^{2i\pi xz/16384} |\underline{z}\rangle$.

  On obtient donc le qbit suivant

$$\begin{aligned}|\varphi_4\rangle = \frac{1}{\sqrt{2731}} \frac{1}{\sqrt{16384}}( & \\ & \sum_{z=0}^{16383} e^{2i\pi 2z/16384} |\underline{z}\rangle + \\ & \sum_{z=0}^{16383} e^{2i\pi 8z/16384} |\underline{z}\rangle + \\ & \cdots + \\ & \sum_{z=0}^{16383} e^{2i\pi 16376z/16384} |\underline{z}\rangle + \\ & \sum_{z=0}^{16383} e^{2i\pi 16382z/16384} |\underline{z}\rangle) \otimes |\underline{74}\rangle\end{aligned}$$

On le met sous la forme

$$|\varphi_4\rangle = \frac{1}{\sqrt{q2^m}} \sum_{z=0}^{2^m-1} \left( \sum_{k=0}^{q} \omega^{krz} \right) \omega^{yz} |\underline{z}\rangle \otimes |\underline{a^y \mod n}\rangle$$

(attention, différence notable avec le cours : la somme de $k$ va jusqu'à $q = \lfloor 2^m/r \rfloor$ et non $q-1$ puisqu'il y a $q+1$ éléments dans le paquet ; puisque, encore une fois $r$ ne divise pas $2^m$)

$$\begin{aligned}
|\varphi_4\rangle = \frac{1}{\sqrt{2731}} \frac{1}{\sqrt{16384}} ( & \\
& \sum_{z=0}^{16383} \left( e^{2i\pi \cdot 0 \cdot 6 \cdot z/16384} \right) e^{2i\pi 2z/16384} |\underline{z}\rangle + \\
& \sum_{z=0}^{16383} \left( e^{2i\pi \cdot 1 \cdot 6 \cdot z/16384} \right) e^{2i\pi 2z/16384} |\underline{z}\rangle + \\
& \cdots + \\
& \sum_{z=0}^{16383} \left( e^{2i\pi \cdot 2729 \cdot 6 \cdot z/16384} \right) e^{2i\pi 2z/16384} |\underline{z}\rangle + \\
& \sum_{z=0}^{16383} \left( e^{2i\pi \cdot 2730 \cdot 6 \cdot z/16384} \right) e^{2i\pi 2z/16384} |\underline{z}\rangle ) \qquad \otimes |\underline{74}\rangle \\
= \frac{1}{\sqrt{2731}} & \sum_{z=0}^{16383} \left( e^{2i\pi \cdot 0 \cdot 6 \cdot z/16384} + e^{2i\pi \cdot 1 \cdot 6 \cdot z/16384} + \cdots + e^{2i\pi \cdot 2730 \cdot 6 \cdot z/16384} \right) e^{2i\pi 2z/16384} |\underline{z}\rangle \quad \otimes |\underline{74}\rangle
\end{aligned}$$

- On fait ensuite une mesure de $z$. Il faut donc estimer la mesure. Dans le cours, il est dit que les $z$ les plus proches de multiples de $\frac{2^m}{r}$ devraient sortir avec une plus forte probabilité. Mesurons cette probabilité autours de ces multiples :

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $k \cdot 2^m/r$ | 0 | 2730.66 | 5461.33 | 8192 | 10922.66 | 13653.33 |

La probabilité de mesurer $z$ est $\left| \frac{1}{\sqrt{2731}} \left( \sum_{k=0}^{2730} e^{2i\pi \cdot k \cdot 6 \cdot z/16384} \right) e^{2i\pi 2z/16384} \right|^2$.

| $z$ | 0 | 1 | 2729 | 2730 | 2731 | 2732 | 5460 | 5461 | 5462 | 5463 |
|---|---|---|---|---|---|---|---|---|---|---|
| Mesure | 0.16 | 2e-9 | 0.005 | 0.028 | 0.11 | 0.007 | 0.007 | 0.11 | 0.028 | 0.005 |
| $z$ | 8191 | 8192 | 8193 | 10921 | 10922 | 10923 | 10924 | | | |
| Mesure | 2e-9 | 0.16 | 2e-9 | 0.004 | 0.028 | 0.11 | 0.007 | | | |
| $z$ | 13652 | 13653 | 13654 | 13655 | | | | | | |
| Mesure | 0.007 | 0.11 | 0.028 | 0.004 | | | | | | |

On observe une régularité dans les probabilités qui dépend de la proximité avec les multiples de $2^m/r$. Il y a environ 76% de chance de mesurer une des 7 valeurs les plus proches de ces multiples. Les autres probabilités sont très petites mais assez nombreuses pour cumuler environ 24%.

- Supposons que la mesure de $z$ donne 0; dans ce cas, on recommence le circuit quantique.

- Supposons maintenant que $z$ donne 8192. Divisons $z$ par $2^m$.

$$\frac{z}{2^m} = \frac{8192}{16384} = \frac{1}{2}$$

On obtient directement un développement en fraction continue. Malheureusement le dénominateur est 2. Et on peut aisément vérifier que $r \neq 2$. En effet $23^2 \not\equiv 1 \mod 91$. On doit donc recommencer le circuit quantique.

- Supposons qu'on mesure $z = 2732$.

$$\frac{z}{2^m} = \frac{2732}{16384} = \frac{1}{5 + \frac{1}{1+\frac{1}{340+\frac{1}{2}}}}$$

On obtient un développement en fraction continue non trivial. On calcule les termes du développement. On prend ensuite la dernière fraction où le dénominateur est plus petit que $n = 91$. Note : le développement en fraction continue n'est pas au programme du cours car on est vite passé dessus, mais il me semblait intéressant de détailler comment procéder. Le cours dit que la fraction qu'on va obtenir est $k/r$ où $k$ est tel que 2732 est proche du multiple $k2^m/r$. Donc ici $k = 1$ (puisque 2732 est proche de 2730.66. Donc on devrait voir 1 / 6 apparaître.)

$$\begin{aligned}
\frac{1}{5} &= \frac{1}{5} \\
\frac{1}{5 + \frac{1}{1}} &= \frac{1}{6} \\
\frac{1}{5 + \frac{1}{1+\frac{1}{340}}} &= \frac{341}{2045} \\
\frac{1}{5 + \frac{1}{1+\frac{1}{340+\frac{1}{2}}}} &= \frac{683}{4096} = \frac{2732}{16384}
\end{aligned}$$

La fraction à considérer est bien $\frac{1}{6}$ comme prévu. Attention : notez qu'on pouvait deviner qu'on allait tomber sur $\frac{1}{6}$ uniquement parce qu'on connait $r$ dans cet exemple. Mais si on n'a aucune connaissance préalable sur $r$ (ce qui est supposé sinon on n'exécuterait pas cet algorithme), on ne pouvait pas connaître cette fraction en avance.

Le dénominateur est 6. On peut constater que $23^6 \equiv 1 \mod 91$. Donc 6 est bien l'ordre de 23. On termine l'algorithme en exchibant $p$ et $q$ comme expliqué au début.

- Supposons enfin qu'on mesure un autre entier loin des multiples de $2^m/r$, par exemple 3330.

$$\frac{z}{2^m} = \frac{3330}{16384} = \frac{1}{4 + \frac{1}{1+\frac{1}{11+\frac{1}{1+\frac{1}{1+\frac{1}{12+\frac{1}{1+\frac{1}{4}}}}}}}}$$

Les termes successifs sont

$$\begin{aligned}
\frac{1}{4} &= \frac{1}{4} \\
\frac{1}{4+\frac{1}{1}} &= \frac{1}{5} \\
\frac{1}{4+\frac{1}{1+\frac{1}{11}}} &= \frac{12}{59} \\
\frac{1}{4+\frac{1}{1+\frac{1}{11+\frac{1}{1}}}} &= \frac{13}{64} \\
\frac{1}{4+\frac{1}{1+\frac{1}{11+\frac{1}{1+\frac{1}{1}}}}} &= \frac{25}{123} \\
\frac{1}{4+\frac{1}{1+\frac{1}{11+\frac{1}{1+\frac{1}{1+\frac{1}{12}}}}}} &= \frac{313}{1540} \\
\frac{1}{4+\frac{1}{1+\frac{1}{11+\frac{1}{1+\frac{1}{1+\frac{1}{12+\frac{1}{1}}}}}}} &= \frac{338}{1663} \\
\frac{1}{4+\frac{1}{1+\frac{1}{11+\frac{1}{1+\frac{1}{1+\frac{1}{12+\frac{1}{1+\frac{1}{4}}}}}}}} &= \frac{1665}{8192} = \frac{3330}{16384}
\end{aligned}$$

La dernière fraction où le dénominateur est plus petit que $n$ est 13/64. On peut constater que le dénominateur n'est pas $r$ puisque $a^r = 23^{64} \equiv 16 \mod 91$.