Solution de la série 10
Traitement Quantique de l'Information

Exercice 1 *Effet de la décohérence dans l'algorithme de Shor*

1. Après les portes de Hadamard :

$$\begin{aligned}
&\widetilde{H}_0 \otimes \widetilde{H}_1 \otimes \mathbb{I} \otimes \mathbb{I}(|0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle) \\
&\qquad = \left(\frac{1}{\sqrt{2}}\right)^2 (|0\rangle + e^{i\varphi_0}|1\rangle) \otimes (|0\rangle + e^{i\varphi_1}|1\rangle) \otimes |0\rangle \otimes |0\rangle \\
&\qquad = \frac{1}{\sqrt{4}}(|00\rangle + e^{i\varphi_0}|10\rangle + e^{i\varphi_1}|01\rangle + e^{i(\varphi_0+\varphi_1)}|11\rangle) \otimes |00\rangle \\
&\qquad = \frac{1}{\sqrt{4}}(|0\rangle + e^{i\varphi_1}|1\rangle + e^{i\varphi_0}|2\rangle + e^{i(\varphi_0+\varphi_1)}|3\rangle) \otimes |0\rangle
\end{aligned}$$

2. Après U_f on obtient l'état :

$$\frac{1}{\sqrt{4}}(|0\rangle \otimes |f(0)\rangle + e^{i\varphi_1}|1\rangle \otimes |f(1)\rangle + e^{i\varphi_0}|2\rangle \otimes |f(2)\rangle + e^{i(\varphi_0+\varphi_1)}|3\rangle \otimes |f(3)\rangle)$$

Puisque $f(x) = f(x+2)$ on a :

$$\frac{1}{\sqrt{4}}(|0\rangle + e^{i\varphi_0}|2\rangle) \otimes |f(0)\rangle + \frac{1}{\sqrt{4}}(e^{i\varphi_1}|1\rangle + e^{i(\varphi_0+\varphi_1)}|3\rangle) \otimes |f(1)\rangle$$

Appliquons la QFT à chaque terme :

$$\frac{1}{4}\sum_{y=0}^{3}(1 + e^{i(\varphi_0+\frac{\pi}{2}2y)})|y\rangle \otimes |f(0)\rangle + \frac{1}{4}\sum_{y=0}^{3}(e^{i(\varphi_1+\frac{\pi}{2}y)} + e^{i(\varphi_0+\varphi_1+\frac{\pi}{2}3y)})|y\rangle \otimes |f(1)\rangle$$

3. L'état juste après la mesure est :

$$|\psi_{post}\rangle = \frac{1}{4}(1 + e^{i(\varphi_0+\pi y)})|y\rangle \otimes |f(0)\rangle + \frac{1}{4}e^{i(\varphi_1+\frac{\pi}{2}y)}(1 + e^{i(\varphi_0+\pi y)})|y\rangle \otimes |f(1)\rangle.$$

La probabilité de l'obtenir est donné par sa norme (au carré)

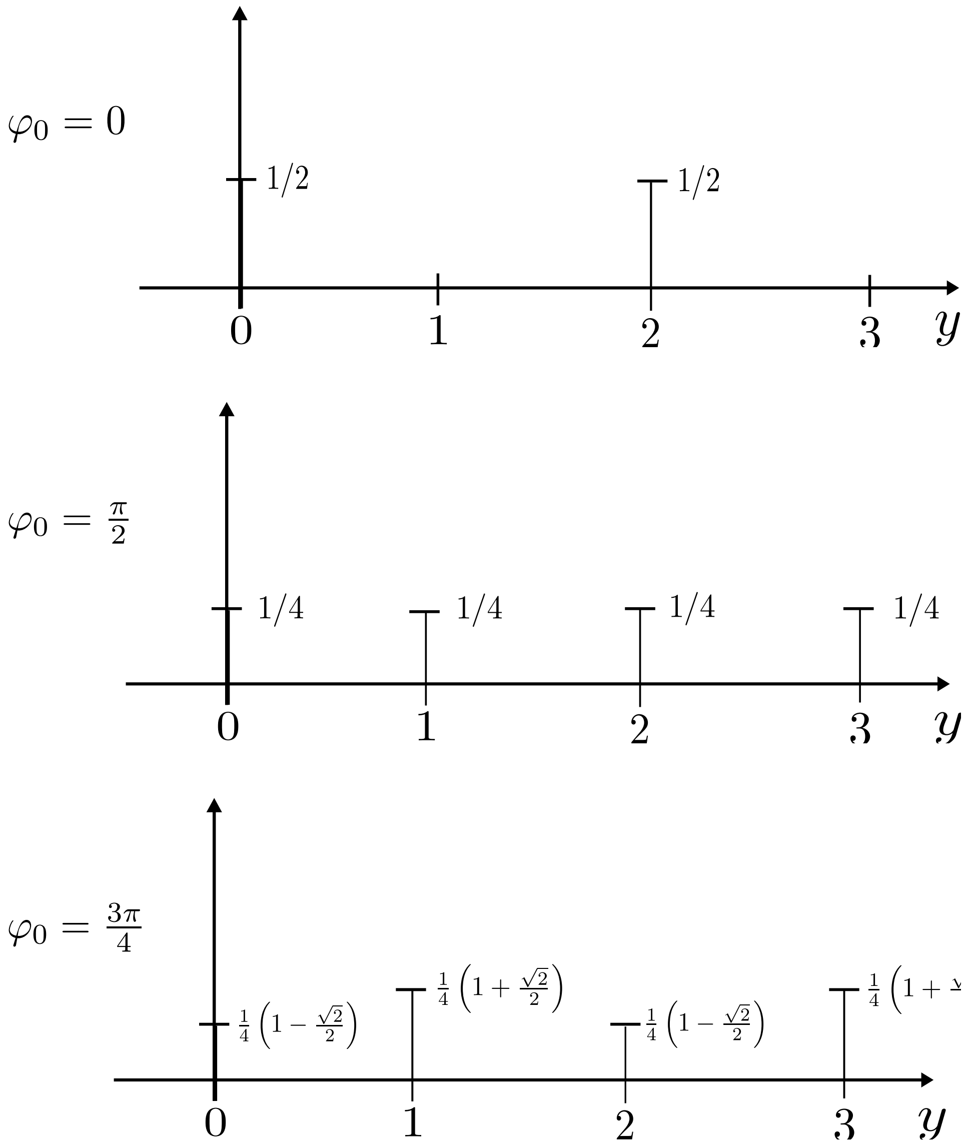
$$
\begin{aligned}
\mathrm{Prob}(y|\varphi_0,\varphi_1) &= \frac{1}{16}\left\{|1+e^{i(\varphi_0+\pi y)}|^2 + |1+e^{i(\varphi_0+\pi y)}|^2\right\} \\
&= \frac{1}{8}\left((1+\cos(\varphi_0+\pi y))^2 + \sin^2(\varphi_0+\pi y)\right)
\end{aligned}
$$

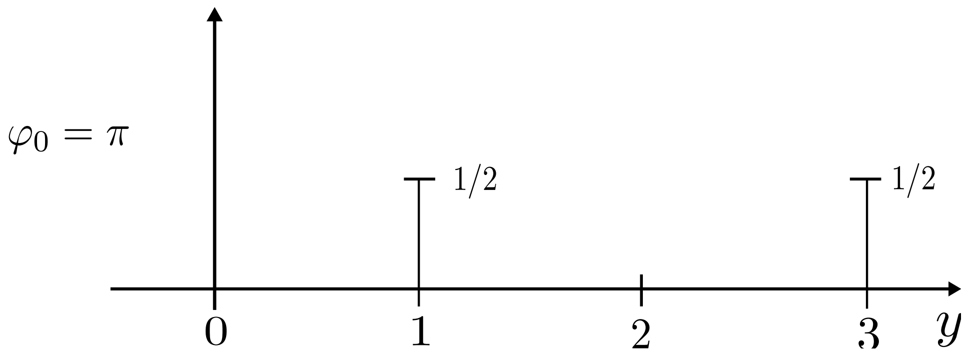
$\Rightarrow$

$$
\mathrm{Prob}(y|\varphi_0,\varphi_1) = \frac{1}{4}\left(1+\cos(\varphi_0+\pi y)\right)
$$

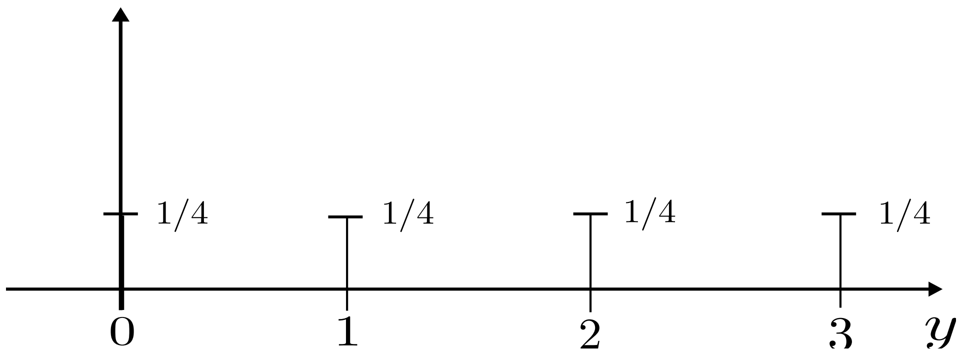
On voit que curieusement cette probabilité ne depend pas de φ_1. Donc l'algorithme de Shor a l'air robuste par rapport à ce déphasage.

4.





$$\text{Prob}(y) = \int \mathrm{d}\varphi_0 \, \text{Prob}(y|\varphi_0) \, \text{Prob}(\varphi_0) = \int_0^{2\pi} \frac{\mathrm{d}\varphi_0}{2\pi} \, \text{Prob}(y|\varphi_0) = \frac{1}{4}$$



Exercice 2

(a) On calcule $7^0 = 1 \mod 15$, $7^1 = 7 \mod 15, 7^2 = 49 = 19 = 4 \mod 15$, $7^3 = 28 = 13 \mod 15$ et $7^4 = 91 = 31 = 1 \mod 15$. Donc, $\text{Ord}_{15}(7) = 4$.

(b) On vérifie que l'ordre $r = 4$ est pair et que $a^{r/2} \neq -1 \mod 15$. En effet $a^{r/2} = 7^2 = 49 = 4 \neq -1 \mod 15$ (car $-1 = 14 \mod 15$). Donc

$$0 = (7^4 - 1) = (7^2 - 1)(7^2 + 1) \mod 15$$

et puisque $7^2 + 1 \neq 0 \mod 15$ il faut que une partie de 15 divise $7^2 - 1$ et une autre partie de 15 divise 7^2+1. En d'autre termes $\text{PGCD}(7^2-1, 15)$ et $\text{PGCD}(7^2+1, 15)$ sont non triviaux.

$$\begin{aligned}
\text{PGCD}(7^2 - 1, 15) &= \text{PGCD}(48, 15) = \text{PGCD}(48 - 15, 15) \\
&= \text{PGCD}(48 - 30, 15) = \text{PGCD}(48 - 45, 15) \\
&= \text{PGCD}(3, 15) = 3
\end{aligned}$$

et

$$\text{PGCD}(7^2 + 1, 15) = \text{PGCD}(50, 15) = \text{PGCD}(50 - 3 \times 15, 15) = \text{PGCD}(5, 15) = 5.$$

Les facteurs premiers de 15 sont donc 3 et 5.

(c) On prend $M = 2^{11} = 2048$, c'est à dire qu' il y a 11 bits dans le premier registre et un certain nombre de bits dans le deuxième registre (on peut prendre 11 mais on en fait on peut faire beaucoup mieux car $f(x)$ prend seulement 4 valeurs comme vu en (a). Donc 2 bits auxiliaires suffisent pour coder $f(x) \in \{1, 7, 4, 13\}$).

(c1) Après les portes de Hadamard l'état est :

$$\frac{1}{\sqrt{2^{11}}} \sum_{x=0}^{2^{11}-1} |x\rangle \otimes |0\rangle.$$

(c2) Après U_f l'état est :

$$\frac{1}{\sqrt{2^{11}}} \sum_{x=0}^{2^{11}-1} |x\rangle \otimes |f(x)\rangle.$$

qui est égal à

$$\begin{aligned} \frac{1}{\sqrt{2^{11}}} \{ & |0\rangle \otimes |1\rangle + |1\rangle \otimes |7\rangle + |2\rangle \otimes |4\rangle + |3\rangle \otimes |13\rangle \\ & |4\rangle \otimes |1\rangle + |5\rangle \otimes |7\rangle + |6\rangle \otimes |4\rangle + |7\rangle \otimes |13\rangle \\ & |8\rangle \otimes |1\rangle + |9\rangle \otimes |7\rangle + |0\rangle \otimes |4\rangle + |11\rangle \otimes |13\rangle \\ & \cdots \} \end{aligned}$$

Dans l'intervalle $[0, 2^{11}]$ on peut mettre $\frac{2^{11}}{4} = 2^9 = 512$ fois la période de longueur 4. Donc cet état sécrit aussi :

$$= \frac{1}{\sqrt{2^11}} \sum_{j=0}^{2^9-1} (|4j\rangle \otimes |1\rangle + |1+4j\rangle \otimes |7\rangle + |2+4j\rangle \otimes |4\rangle + |3+4j\rangle \otimes |13\rangle).$$

(c3) Appliquons la QFT à cette somme. Pour chaque terme on a :

$$\mathrm{QFT}|x_0 + 4j\rangle = \frac{1}{\sqrt{2^{11}}} \sum_{y=0}^{2^{11}-1} e^{2\pi i \frac{(x_0+4j)y}{2^{11}}} |y\rangle$$

avec $x_0 = 0, 1, 2$ et 3.
En remplacant on trouve la formule (voir cours) :

$$\frac{1}{\sqrt{2^{11}}} \sum_{x_0=0}^{3} \left\{ \sum_{y=0}^{2^{11}-1} e^{2\pi i \frac{x_0 y}{2^11}} \sum_{j=0}^{2^9-1} e^{2\pi i \frac{j\,y}{2^9}} |y\rangle \right\} \otimes |f(x_0)\rangle$$

ou $|f(x_0)\rangle$ vaut respectivement $|1\rangle$; $|7\rangle$; $|4\rangle$; $|13\rangle$.

(c4) La fonction $\Pr(y)$ vaut :

$$\begin{aligned} \Pr(y) &= \frac{1}{(2^{11})^2} \sum_{x_0=0}^{3} \left| \sum_{j=0}^{2^9-1} e^{2\pi i \frac{j\,y}{2^9}} \right|^2 \\ &= \frac{4}{2^{22}} \left| \sum_{j=0}^{511} e^{2\pi i \frac{jy}{512}} \right|^2. \end{aligned}$$

Essayons les valeus $y = 0, y = 512, y = 2 \times 512 = 1024$ et $y = 3 \times 512 = 1536$. On trouve pour ces 4 valeurs

$$\text{Prob}(y) = \frac{2^2}{2^{22}}.(2^9)^2 = \frac{2^2}{2^{22}}.2^{18} = \frac{1}{4}.$$

Donc pour toutes les autres valeus on doit avoir $\text{Prob}(y) = 0$. C'est à dire que la mesure va certainement donner une des 4 valeurs

$$y \in \{0, 512, 1024, 1536\}.$$

(c5) Supposons que la mesure donne $y = 1536$. Alors on a

$$\frac{y}{M} = \frac{1536}{1048} = \frac{3}{4}.$$

Ainsi le dénominateur 4 est un candidat pour r. On essaye $\Omega = 4$. On fait une vérification $a^r = 7^4 = \cdots = 1 \bmod 15$. $\Longrightarrow$ SUCCES. (En fait ici la mesure y correspond à $k = 3$ qui est premier avec $r = 4$: c'est pour cela que l'on a un succès).

(c6) Supposons que la mesure donne $y = 0$. On ne peut rien tirer pour r car $\frac{y}{M} = 0 = \frac{k}{\omega}$ pour $k = 0$ et r est quelconque. ECHEC

1. Supposons que la mesure donne $y = 512$. Alors

   $$\frac{y}{M} = \frac{512}{2048} = \frac{2^9}{2^{11}} = \frac{1}{2^2} = \frac{1}{4}.$$

   le dénominaeur est $r = 4$. On vérifie $a^r = 7^4 = 1 \bmod 15$ SUCCES. (En fait ici la mesure y correspond à $k = 1$ qui est premier avec $r = 4$: c'est pour cela que l'on a un succès).

2. Supposons

   $$\frac{y}{M} = \frac{1024}{2048} = \frac{1}{2}.$$

   Ici le dénominateur est 2. On essaye $r = 2$ en vérifiant $ar = 7^2 = 49 = 3 \neq 1 \bmod 15$ $\Longrightarrow$ ECHEC. $r = 2$ ne peut pas être le bon résultat. (En fait ici la mesure donne un y qui correspond à $k = 2$ et ce nombre n'est pas premier avec $r = 4$: c'est pour cela que l'on a un échec.)

Exercice 3

La transformée de Fourier quantique agit sur les vecteurs de base

$$|x\rangle \in \{|0\rangle, |1\rangle, \cdots |M-1\rangle\}$$

comme suit :

$$\text{QFT } |x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} |y\rangle.$$

(a) $M = 2$:

$$\begin{aligned}
\text{QFT } |x\rangle &= \frac{1}{\sqrt{2}}\left(e^{2\pi i \frac{x\cdot 0}{2}}|0\rangle + e^{2\pi i \frac{x\cdot 1}{2}}|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi x}|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^x|1\rangle\right)
\end{aligned}$$

On reconnait que $\text{QFT}|x\rangle = H|x\rangle$ si $M = 2$.

(b) $M = 4$:

$$\begin{aligned}
\text{QFT } |x\rangle &= \frac{1}{\sqrt{4}}\left(e^{2\pi i \frac{x\cdot 0}{4}}|0\rangle + e^{2\pi i \frac{x\cdot 1}{4}}|1\rangle + e^{2\pi i \frac{x\cdot 2}{4}}|2\rangle + e^{2\pi i \frac{x\cdot 3}{4}}|3\rangle\right) \\
&= \frac{1}{2}\left(|0\rangle + (i)^x|1\rangle + (-1)^x|2\rangle + (-i)^x|3\rangle\right) \\
&= \frac{1}{2}\left\{\left(|0\rangle + (i)^x|1\rangle\right) + (-1)^x\left(|2\rangle + (i)^x|3\rangle\right)\right\}
\end{aligned}$$

Notez la structure hiérarchique :

$$\frac{1}{\sqrt{2}}\left\{\underbrace{\frac{1}{\sqrt{2}}\left(|0\rangle + (i)^x|1\rangle\right)}_{|\widetilde{0}\rangle} + (-1)^x \underbrace{\frac{1}{\sqrt{2}}\left(|2\rangle + (i)^x|3\rangle\right)}_{|\widetilde{1}\rangle}\right\}$$

(c) Il suffit de montrer que l'orthogonalité de la base computationnelle $|x\rangle$ est préservée.

$$\begin{aligned}
\langle x'|(\text{QFT})^\dagger &= \frac{1}{\sqrt{M}}\sum_{y'=0}^{M-1} e^{-2\pi i \frac{x'y'}{M}}\langle y'| \\
\Rightarrow \quad \langle x'|(\text{QFT})^\dagger(\text{QFT})|x\rangle &= \frac{1}{M}\sum_{y'=0}^{M-1}\sum_{y=0}^{M-1} e^{-2\pi i \frac{x'y'}{M}} e^{2\pi i \frac{xy}{M}}\langle y'|y\rangle
\end{aligned}$$

Grâce à $\langle y'|y\rangle = \delta_{y'y}$ on obtient :

$$\langle x'|(\text{QFT})^\dagger(\text{QFT})|x\rangle = \frac{1}{M}\sum_{y=0}^{M-1} e^{-2\pi i \frac{(x'-x)}{M}y}$$

– Cette expression est trivialement égale à 1 si $x' = x$.

– Si $x' \neq x$ une façon de la calculer est de reconnaitre la série géométrique :

$$\begin{aligned}
\frac{1}{M}\sum_{y=0}^{M-1} e^{2\pi i \frac{(x-x')}{M} y} &= \frac{1}{M}\sum_{y=0}^{M-1} \left(e^{2\pi i \frac{(x-x')}{M}}\right)^{y} \\
&= \frac{1}{M}\frac{1-\left(e^{2\pi i \frac{(x-x')}{M}}\right)^{M}}{1-e^{2\pi i \frac{(x-x')}{M}}} \\
&= \frac{1}{M}\frac{1-1}{1-e^{2\pi i \frac{(x-x')}{M}}} \\
&= 0.
\end{aligned}$$

Finalement, on trouve $\langle x'|(\mathrm{QFT})^{\dagger}(\mathrm{QFT})|x\rangle = \delta_{xx'} = \langle x'|x\rangle$