ENSEIRB-MATMECA
Option second semestre, 2015/2016

Information Quantique

Corrigé de l'examen du 17 Mai 2016

Exercice 1 (/10 pts)
Interféromètre de Mach-Zehnder.

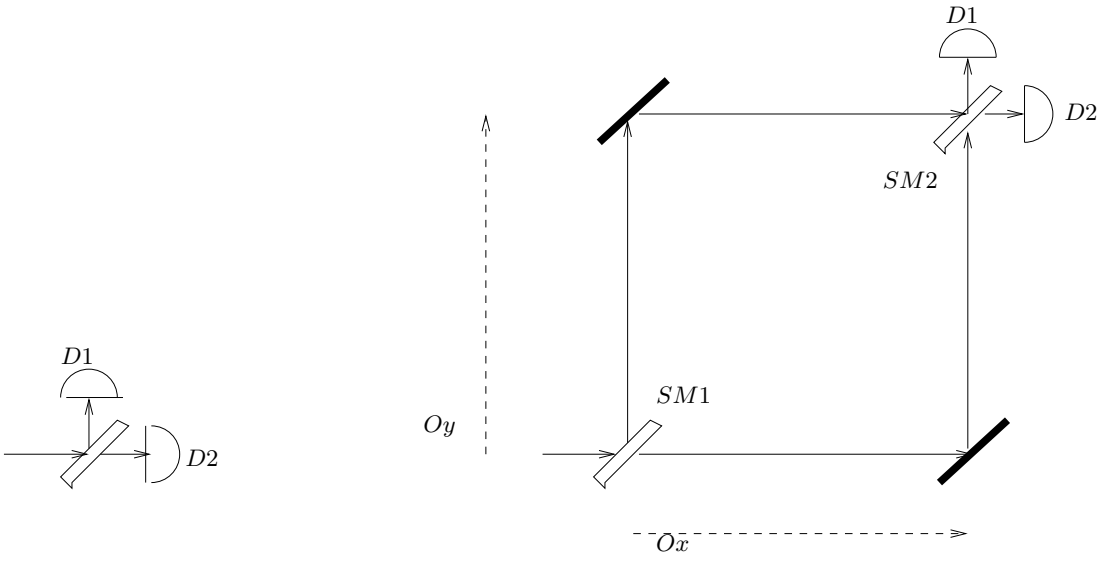

FIGURE 1 – Interféromètre de Mach-Zehnder.

1- La transformation unitaire décrivant le passage du photon à travers la lame semi-réfléchissante est (selon l'énoncé) $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}$. Létat du photon après la première lame ($SM1$) est donc :

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\cdot\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{i}{\sqrt{2}}\end{pmatrix}$$

La transformation unitaire décrivant le passage du photon à travers les miroirs est (selon l'énoncé) $\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$. Létat du photon après le passage dans le

couple de miroirs est donc :

$$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}$$

L'état du photon après la seconde lame ($SM2$) est :

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

2- L'état du photon après la seconde lame exprime un déplacement horizontal du photon vers le détecteur D_2 (avec une phase (-1)). Autrement dit, l'état du photon est un état *propre* de l'observable associé aux détecteurs (D_1, D_2). Donc *avec probabilité* 1, on mesure le passage du photon dans D_2. Le photon arrive dans le détecteur D_1 avec probabilité 0

Plaçons-nous dans le cas où un observateur mesure le passage du photon par le trajet de gauche (resp. de droite) après le miroir et juste avant la seconde lame semi-réfléchissante. Il utilise une observable dont les deux vecteurs propres sont $|x\rangle$ (cas où le photon est passé à gauche), et $|y\rangle$ (cas où le photon est passé à droite).
Rappelons que l'état du photon juste avant la mesure (du trajet choisi) est

$$|e\rangle = \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}$$

3- **cas où le photon passe à gauche** :
Ce cas se produit avec une probabilité égale à $|\langle x|e\rangle|^2 = \frac{1}{2}$
L'etat après cette mesure est $|x\rangle$. L' état après cette mesure, puis le passage dans SM2 est :

$$|e'\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \cdot |x\rangle = \frac{1}{\sqrt{2}}(|x\rangle + i\,|y\rangle)$$

Il passe dans D_1 avec probabilité :

$$|\langle y|e'\rangle|^2 = \frac{1}{2}$$

et dans D_2 avec probabilité :

$$|\langle x|e'\rangle|^2 = \frac{1}{2}.$$

cas où le photon passe à droite :
Ce cas se produit avec une probabilité égale à $|\langle y|e\rangle|^2 = \frac{1}{2}$
L'etat après cette mesure est $|y\rangle$. L'état après cette mesure, puis le passage dans SM2 est :

$$\left|e''\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\cdot|y\rangle = \frac{1}{\sqrt{2}}(i\,|x\rangle + |y\rangle)$$

Il passe dans D_1 avec probabilité :

$$|\left\langle y|e''\right\rangle|^2 = \frac{1}{2}$$

et dans D_2 avec probabilité :

$$|\left\langle x|e''\right\rangle|^2 = \frac{1}{2}.$$

Finalement le photon est détecté dans D_1 :
- soit après avoir pris le trajet de gauche ($\Pr = \frac{1}{2}$) puis avoir traversé la lame semi-réfléchissante vers D_1 ($\Pr = \frac{1}{2}$) : ce cas survient avec probabilité $\frac{1}{4}$.
- soit après avoir pris le trajet de droite ($\Pr = \frac{1}{2}$) puis avoir traversé la lame semi-réfléchissante vers D_1 ($\Pr = \frac{1}{2}$) : ce cas survient avec probabilité $\frac{1}{4}$.
Le photon est détecté dans D_1 avec probabilité $\frac{1}{2}$.
Le photon est détecté dans D_2 avec probabilité $1 - \frac{1}{2} = \frac{1}{2}$.
Si l'on reproduit N fois cette expérience (avec un observateur qui mesure le passage du photon par la gauche ou la droite) le photon sera détecté en moyenne $N/2$ fois en D_1, et $N/2$ fois en D_2.
N.B. Le phénomène d'"auto-interférence" a *disparu*.
4- L'opérateur d'évolution du système décrivant A a pour matrice, dans la base $|x\rangle, |y\rangle$ (de l' espace des états de A)

$$\frac{-1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\cdot\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\cdot\frac{-1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

L'opérateur d'vólution du système décrivant A' a la même matrice, dans la base $|x'\rangle, |y'\rangle$ (de l' espace des états de A'). L'opérateur d'évolution du système décrivant (A, A') est le produit tensoriel de ces deux opérateurs :

$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\otimes\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$

L'état du sytème (A, A') après la traversée des deux appareils est donc

$$(\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\otimes\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix})\cdot(|x\rangle\otimes\left|x'\right\rangle) = \begin{pmatrix}-1\\ 0\end{pmatrix}\otimes\begin{pmatrix}-1\\ 0\end{pmatrix} = |x\rangle\otimes\left|x'\right\rangle.$$

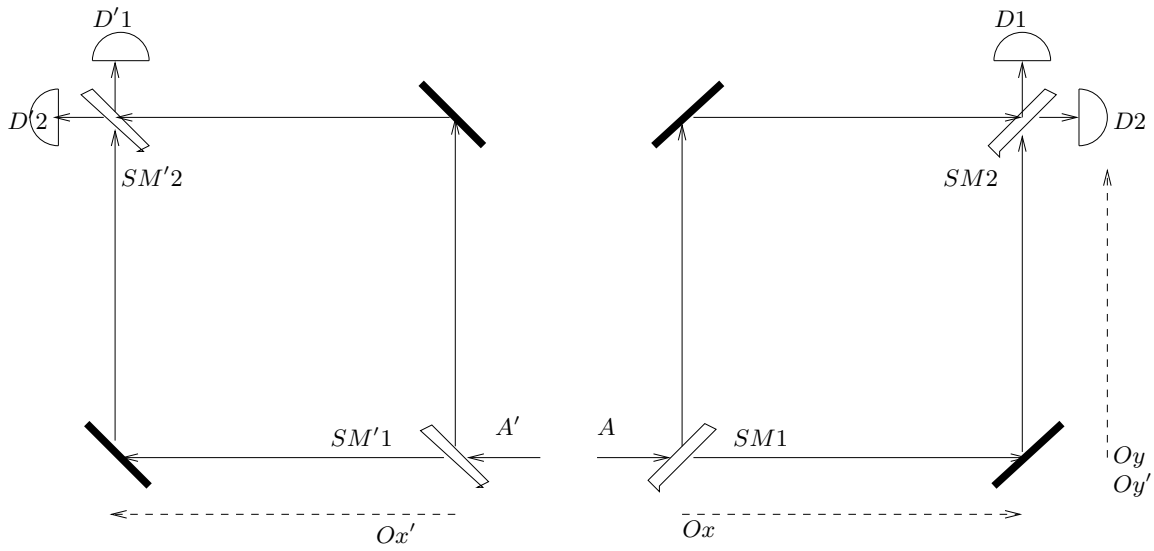

FIGURE 2 – Deux interféromètres de Mach-Zehnder.

Donc, avec probabilité 1, l'observateur du côté de A verra A passer dans D_2 et l'observateur du côté de A' verra A' passer dans D'_2.

Examinons les idées de Cosinus.
5- Dans son scénario, l'état initial du système (A, A') est

$$\frac{1}{\sqrt{2}}(|x\rangle \otimes |x'\rangle + |y\rangle \otimes |y'\rangle).$$

Après le passage dans le miroir, l'état du système (A, A') est :

$$\begin{aligned} & \left(\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\right) \cdot \frac{1}{\sqrt{2}}(|x\rangle \otimes |x'\rangle + |y\rangle \otimes |y'\rangle) \\ = \quad & \frac{-1}{\sqrt{2}}(|y\rangle \otimes |y'\rangle + |x\rangle \otimes |x'\rangle). \end{aligned}$$

6- 6.1 **cas où Cosinus ne fait pas de mesure** (il "transmet" 0),
L'état du système (A, A'), sans mesure de Cosinus (s'il transmet 0), avant $SM2$ est l'état obtenu en Q5 :

$$\frac{-1}{\sqrt{2}}(|y\rangle \otimes |y'\rangle + |x\rangle \otimes |x'\rangle).$$

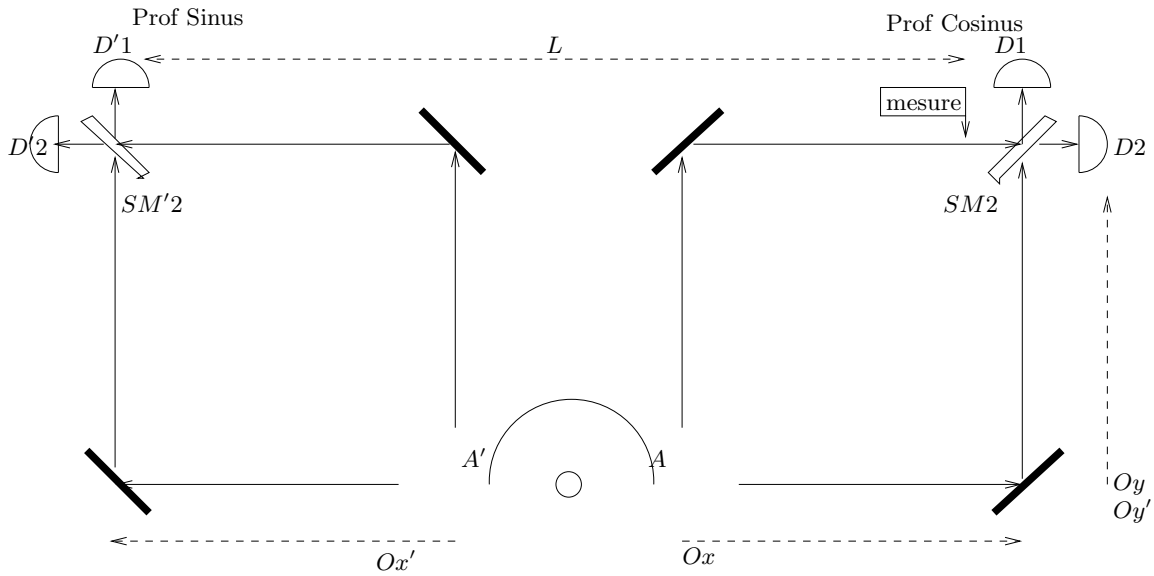

FIGURE 3 – Photons intriqués dans Mach-Zehnder.

L'état obtenu après $SM2$ est :

$$\begin{aligned}
& \frac{1}{2}\left(\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\otimes\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\right)\cdot\frac{-1}{\sqrt{2}}(|y\rangle\otimes|y'\rangle+|x\rangle\otimes|x'\rangle)\\
= & \frac{-1}{2\sqrt{2}}[(|x\rangle+i\,|y\rangle)\otimes(|x'\rangle+i\,|y'\rangle)+(i\,|x\rangle+|y\rangle)\otimes(i\,|x'\rangle+|y'\rangle)]\\
= & \frac{-1}{2\sqrt{2}}[2i(|x\rangle\otimes|y'\rangle)+2i(|y\rangle\otimes|x'\rangle)]\\
= & \frac{-i}{\sqrt{2}}[|x\rangle\otimes|y'\rangle+|y\rangle\otimes|x'\rangle]
\end{aligned}$$

6.2 **cas où Cosinus fait une mesure** (il "transmet" 1),
L'état du système (A, A'), avant la mesure de Cosinus est l'état obtenu en Q5 :

$$\frac{-1}{\sqrt{2}}(|y\rangle\otimes|y'\rangle+|x\rangle\otimes|x'\rangle).$$

L'état du système (A, A'), après la mesure de Cosinus est :
cas 1 : avec $\Pr=\frac{1}{2}$

$$(-1)\,|x\rangle\otimes|x'\rangle$$

cas 2 : avec $\Pr = \frac{1}{2}$

$$(-1)\left|y\right\rangle \otimes \left|y'\right\rangle .$$

L'état du système (A, A') avant $SM2$ est celui donné ci-dessus.
L'état du système (A, A') après $SM2$ est :
dans le cas 1

$$\begin{aligned} & \frac{-1}{2}(\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}) \cdot (\left|x\right\rangle \otimes \left|x'\right\rangle) \\ = & \frac{-1}{2}(\left|x\right\rangle + i\left|y\right\rangle) \otimes (\left|x'\right\rangle + i\left|y'\right\rangle) \\ = & \frac{-1}{2}[\left|x\right\rangle \left|x'\right\rangle + i\left|y\right\rangle \left|x'\right\rangle + i\left|x\right\rangle \left|y'\right\rangle - \left|y\right\rangle \left|y'\right\rangle] \end{aligned}$$

dans le cas 2

$$\begin{aligned} & \frac{-1}{2}(\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}) \cdot (\left|y\right\rangle \otimes \left|y'\right\rangle) \\ = & \frac{-1}{2}(i\left|x\right\rangle + \left|y\right\rangle) \otimes (i\left|x'\right\rangle + \left|y'\right\rangle) \\ = & \frac{1}{2}[\left|x\right\rangle \left|x'\right\rangle - i\left|y\right\rangle \left|x'\right\rangle - i\left|x\right\rangle \left|y'\right\rangle - \left|y\right\rangle \left|y'\right\rangle] \end{aligned}$$

7- Ce qu'observe le professeur Sinus dans le cas où Cosinus "transmet" 0 : il mesure A' avec une observable de vecteurs propres $\left|x'\right\rangle, \left|y'\right\rangle$. Il projette donc l'état du système, avec $\Pr = \frac{1}{2}$ sur :

$$-i\left|y\right\rangle \otimes \left|x'\right\rangle]$$

et voit A' passer dans D'_2
ou alors, avec $\Pr = \frac{1}{2}$ sur :

$$-i\left|x\right\rangle \otimes \left|y'\right\rangle$$

et voit A' passer dans D'_1.
Ce qu'observe le professeur Sinus dans le cas où Cosinus "transmet" 1 **dans le cas 1** :il mesure A' avec une observable de vecteurs propres $\left|x'\right\rangle, \left|y'\right\rangle$. Il projette donc l'état du système, avec $\Pr = \frac{1}{2}$ sur :

$$\frac{1}{\sqrt{2}}[-\left|x\right\rangle \left|x'\right\rangle - i\left|y\right\rangle \left|x'\right\rangle]$$

et voit A' passer dans D'_2
ou alors, avec $\Pr = \frac{1}{2}$ sur :

$$\frac{1}{\sqrt{2}}[-i\,|x\rangle\,|y'\rangle + |y\rangle\,|y'\rangle]$$

et voit A' passer dans D'_1.
dans le cas 2 :un calcul similaire montre que A' est observé dans D'_1 avec $\Pr = \frac{1}{2}$.
Comme les deux cas sont équiprobables, Sinus détecte A' en D'_1 avec probabilité $\frac{1}{2}$.
8- Cosinus a-t-il réussi à transmettre une information à une vitesse deux fois supérieure à celle de la lumière ?
NON : les observations de Sinus ont la même loi de probabilité lorsque Cosinus "transmet 0 " et lorsque Cosinus "transmet 1" :
D'_1 avec $\Pr = \frac{1}{2}$, D'_2 avec $\Pr = \frac{1}{2}$.
Sinus ne peut donc pas déduire de ses mesures une information concernant le choix de Cosinus (transmettre 0 ou transmettre 1).

Exercice 2(/10 pts)

Ordre multiplicatif d'un nombre a modulo N.

On a introduit (dans le cours sur l'algorithme de Shor) l'opérateur U : $\mathcal{B}^{\otimes n} \to \mathcal{B}^{\otimes n}$:

$$\begin{aligned} U\,|x\rangle &:= |a \cdot x \pmod N\rangle \text{ si } 0 \leq x \leq N-1 \\ U\,|x\rangle &:= |x\rangle \text{ si } N \leq x \leq 2^n - 1. \end{aligned}$$

1- U envoie la base canonique sur elle-même, donc U est unitaire.
2.1 Supposons que $U^k = I$.
alors $U^k\,|1\rangle = |1\rangle$. Par ailleurs, $U^k\,|1\rangle = \left|a^k \pmod N\right\rangle$.Donc

$$a^k \equiv 1 \pmod N.$$

2.2 Supposons que $a^k \equiv 1 \pmod N$. Soit $x \in [0, N-1]$. On a $x^k \cdot x \equiv 1 \cdot x \pmod N$ donc $U^k\,|x\rangle = |x\rangle$.
Si $x \in [N, 2^n - 1]$, on a $U^k\,|x\rangle = |x\rangle$ et donc $U^k\,|x\rangle = |x\rangle$. Finalement : $U^k = I$.
3- Comme le polynôme $X^r - 1$ annule U, le spectre de U est inclus dans l' ensemble des zéros de $X^r - 1$, c' est à dire :

$$\{e^{\frac{2i\pi j}{r}} \mid 0 \leq j \leq r-1\}.$$

4- Soit $j \in [0, r-1]$. On note $\omega_j = e^{\frac{2i\pi j}{r}}$.
Calculer le polynôme $D_j \in \mathbb{C}[X]$ tel que

$$X^r - 1 = (X - \omega_j) \cdot D_j.$$

D'après l'identité

$$X^k - Y^k = (X-Y)(X^{k-1}Y^0 + \ldots + X^\ell Y^{k-\ell-1} + + \ldots + X^0 Y^{k-1}).$$

on a

$$X^k - \omega_j^k = (X-\omega_j)(X^{k-1}\omega_j^0 + \ldots + X^\ell \omega_j^{k-\ell-1} + + \ldots + X^0 \omega_j^{k-1}).$$

Donc

$$D_j = (X^{k-1}\omega_j^0 + \ldots + X^\ell \omega_j^{k-\ell-1} + \ldots + X^0 \omega_j^{k-1}).$$

5- On pose $|\varphi_j\rangle := D_j(U) \cdot |1\rangle$.
Comme le polynôme $(X - \omega_j)D_j$ annule U, on a :

$$(U - \omega_j I) \circ D_j(U) = 0$$

donc, pour tout vecteur $|u\rangle$ on a

$$D_j(U) \cdot |u\rangle \in \mathrm{Ker}(U - \omega_j I).$$

Dans le cas du vecteur $|1\rangle$ on a :

$$\begin{aligned} D_j(U) \cdot |1\rangle &= (\sum_{\ell=0}^{r-1} U^\ell \omega_j^{r-\ell-1}) \, |1\rangle \\ &= \sum_{\ell=0}^{r-1} \omega_j^{r-\ell-1}) \left|a^\ell\right\rangle \end{aligned}$$

qui est non-nul : les $\left|a^\ell\right\rangle$ sont des vecteurs deux à deux distincts de la base canonique, donc les coordonnées dans la base canonique de $|\varphi_j\rangle$ sont non-nulles. Donc $|\varphi_j\rangle \neq \overrightarrow{0}$.
On en déduit que le spectre de U est exactement $\{e^{\frac{2i\pi j}{r}} \mid 0 \leq j \leq r-1\}$.
6- Calculons les produits scalaires $\langle \varphi_j | \varphi_k \rangle$ pour $j, k \in [0, r-1]$.

$$\begin{aligned} |\varphi_j\rangle &= \sum_{\ell=0}^{r-1} e^{\frac{-2i\pi j(\ell+1)}{r}} U^\ell \, |1\rangle \\ &= \sum_{\ell=0}^{r-1} e^{\frac{-2i\pi j(\ell+1)}{r}} U^\ell \, |1\rangle \\ &= \sum_{\ell=0}^{r-1} \omega_{\ell+1}^j \left|a^\ell\right\rangle \end{aligned}$$

Sachant que les $\left|a^\ell\right\rangle$ forment ne famille orthonormée, on obtient :

$$\begin{aligned}\langle\varphi_j|\varphi_k\rangle &= \sum_{\ell=0}^{r-1}\overline{\omega_{\ell+1}}^j\omega_{\ell+1}^k \\ &= \sum_{\ell=0}^{r-1}{\omega_{\ell+1}}^{k-j}.\end{aligned}$$

cas 1 : $j=k$
Alors

$$\langle\varphi_j|\varphi_k\rangle = \sum_{\ell=0}^{r-1}1 = r.$$

cas 2 : $j\neq k$
Alors $\omega_{\ell+1}^{k-j}$ annule le polynôme X^r-1 sans annuler $X-1$, donc il annule le quotient $\frac{X^r-1}{X-1}=\sum_{\ell=0}^{r-1}X^\ell$, donc

$$\langle\varphi_j|\varphi_k\rangle = 0.$$

La famille $(|\varphi_j\rangle)_{j\in[0,r-1]}$ est orthogonale et la norme de chacun de ses vecteurs est $\sqrt{r}$. Donc la famille $(|\psi_j\rangle)_{j\in[0,r-1]}$, qui est obtenue en la quotientant par $\sqrt{r}$, est orthonormée.
7- Calculons la somme des vecteurs $|\psi_j\rangle$.

$$\begin{aligned}\sum_{j=0}^{r-1}|\psi_j\rangle &= \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}\omega_j(\sum_{\ell=0}^{r-1}\omega_j^{-\ell-1}U^\ell\,|1\rangle) \\ &= \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}(\sum_{\ell=0}^{r-1}\omega_j^{-\ell}\left|a^\ell\right\rangle) \\ &= \frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1}(\sum_{j=0}^{r-1}\omega_j^{-\ell})\left|a^\ell\right\rangle \qquad (1)\end{aligned}$$

Notons $c(\ell)$ le coefficient de $\left|a^\ell\right\rangle$ dans la somme ci-dessus.
cas 1 : $\ell=0$
Alors

$$c(\ell) = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}\omega_j^0 = \sqrt{r}.$$

cas 2 : $\ell\neq 0$
Alors, par les arguments utilisés à la question 6, $c(\ell)=0$.

En remplaçant dans l'évaluation (1), chaque coefficient $c(\ell)$ par sa valeur, on obtient

$$\sum_{j=0}^{r-1} |\psi_j\rangle = \sqrt{r}\,|1\rangle\,.$$

N.B. Erreur dans le texte donc : le coefficient $\sqrt{r}$ manquait. Mais comme la famille $(|\psi_j\rangle)_{j\in[0,r-1]}$ est orthonormée, sa somme a une norme égale à $\sqrt{r}$, alors que $|1\rangle$ est unitaire ! [1]

8- Appliquons V au vecteur $|0\rangle \otimes |1\rangle \in \mathcal{B}^{\otimes n} \otimes \mathcal{B}^{\otimes n}$; on obtient un état

$$|\eta\rangle := V\,|0\rangle\,|1\rangle\,.$$

Mesurons les n premiers q-bits de cet état : on utilise une observable $\mathcal{O}$ et on obtient un résultat (aléatoire) $y \in [0, 2^n - 1]$. Analysons la loi de y.
Soit $j \in [0, r-1]$.
On a

$$|\eta\rangle = \frac{1}{\sqrt{r}}[|\alpha_1\rangle\,|\psi'_1\rangle + \ldots + |\alpha_\ell\rangle\,|\psi'_\ell\rangle + \ldots + |\alpha_{r-1}\rangle\,|\psi'_{r-1}\rangle\,.$$

Notons $H_j \subseteq \mathcal{B}^{\otimes n}$ le sous-espace propre associé à la valeur propre j de l'observable $\mathcal{O}$. Notons $\mathrm{pr}_{E_j} : \mathcal{B}^{\otimes n} \to \mathcal{B}^{\otimes n}$ la projection orthogonale sur ce sous-espace E_j. On a :

$$(\mathrm{pr}_{E_j} \otimes Id_{2^n})\,|\eta\rangle \;=\; \frac{1}{\sqrt{r}} \cdot \sum_{\ell=0}^{r-1} \mathrm{pr}_{E_j}\,|\alpha_\ell\rangle \otimes |\psi'_\ell\rangle$$

Comme les vecteurs $|\psi'_\ell\rangle$ forment une famille orthonormée, les vecteurs $(\mathrm{pr}_{E_j}\,|\alpha_\ell\rangle) \otimes |\psi'_\ell\rangle$ sont, eux-aussi, orthogonaux deux à deux ; donc

$$\begin{aligned}
\|\mathrm{pr}_{E_j} \otimes Id_{2^n}\,|\eta\rangle\,\|^2 &= \frac{1}{r} \cdot \sum_{\ell=0}^{r-1} \|\mathrm{pr}_{E_j}\,|\alpha_\ell\rangle \otimes |\psi'_\ell\rangle\,\|^2 \\
&= \frac{1}{r} \cdot \sum_{\ell=0}^{r-1} \|\mathrm{pr}_{E_j}\,|\alpha_\ell\rangle\,\|^2 \\
&\geq \frac{1}{r} \cdot \|\mathrm{pr}_{E_j}\,|\alpha_j\rangle\,\|^2 \\
&\geq \frac{1}{r} \cdot \frac{8}{\pi^2}.
\end{aligned}$$

1. mea culpa ; tout étudiant remarquant cette erreur reçoit, bien évidemment, des points supplémentaires.

D'après l' énoncé de Q7, ce carré de norme de projection est la probabilité que la mesure de l'observable $\mathcal{O}$ donne un résultat y vérifiant

$$|\frac{j}{r} - \frac{y}{2^n}| \leq \frac{1}{2^n}.$$

Autrement dit, dans l'état $|\eta\rangle$ on a :

$$\Pr\{|\frac{j}{r} - \frac{y}{2^n}| \leq \frac{1}{2^n}\} \geq \frac{8}{r\pi^2}. \tag{2}$$

Comme, pour des valeurs de j différentes, les événements

$$\{|\frac{j}{r} - \frac{y}{2^n}| \leq \frac{1}{2^n}\}$$

sont disjoints, on en conclut que

$$\begin{aligned} \Pr\{\exists j \in [0, r-1] \mid |\frac{j}{r} - \frac{y}{2^n}| \leq \frac{1}{2^n}\} &\geq \sum_{j=0}^{r-1} \frac{8}{r\pi^2} \\ &= \frac{8}{\pi^2} \end{aligned} \tag{3}$$

9- On répète deux fois le calcul de la question 8 : on obtient deux valeurs $y, y' \in [0, 2^n - 1]$.
Avec une probabilité $\geq \frac{64}{\pi^4}$ (car ces deux calculs sont indépendants) on obtient des y, y' tels que :

$$\exists j, j' \in [0, r-1] \mid |\frac{j}{r} - \frac{y}{2^n}| \leq \frac{1}{2^n} \text{ et } |\frac{j'}{r} - \frac{y'}{2^n}| \leq \frac{1}{2^n}.$$

En supposant que $2^n \geq r^2$, en développant en fraction continue $\frac{y}{2^n}$ puis $\frac{y'}{2^n}$ on obtient, en temps polynomial, des nombres rationnels

$$\frac{j}{r}, \ \frac{j'}{r}.$$

N.B. mais on ne connait pas encore les *couples de nombres* entiers $(j, r).(j', r)$
La proportion de couples (j, j') premiers entre eux dans $[0, n-1]$ tend vers $\frac{6}{\pi^2}$ lorsque n tend vers l'infini. Donc, il existe $r_0 \in \mathsf{N}$ tel que, pour $r \geq r_0$,

$$\text{Card}\{(j, j') \in [0, r-1] \times [0, r-1] \mid j \wedge j' = 1\} \geq \frac{3}{\pi^2} r^2$$

Pour chaque couple $(j, j') \in [0, r-1] \times [0, r-1] \mid j \wedge j' = 1$, la minoration (2) s'applique. On en conclut que, la probabilité que les deux mesures fournissent des rationnels $\frac{j}{r}$, $\frac{j'}{r}$ avec $j \wedge j' = 1$ est plus grande que

$$\frac{8}{\pi^2} \cdot \frac{8}{\pi^2} \cdot \frac{3}{\pi^2}.$$

On suppose désormais que $j \wedge j' = 1$.
Pour tous rationnels

$$s = \prod_{k=1}^{\ell} p_k^{e_k}, \quad t = \prod_{k=1}^{\ell} q_k^{f_k}$$

où les p_k sont des nombres premiers et $e_k, f_k \in \mathbb{Z}$, nous noterons

$$s \wedge t := \prod_{k=1}^{\ell} p_k^{\min(e_k, f_k)}, \quad s \vee t := \prod_{k=1}^{\ell} p_k^{\max(e_k, f_k)}.$$

N.B. lorsque s, t sont entiers , $s \wedge t$ est le pgcd de s, t et $s \vee t$ est le ppcm de s, t.
Supposons que les décompositions de r, j, j' en facteurs premiers sont :

$$r = \prod_{k=1}^{\ell} p_k^{e_k}, \quad j = \prod_{k=1}^{\ell} p_k^{f_k}, \quad j' = \prod_{k=1}^{\ell} p_k^{g_k}.$$

Alors

$$\frac{r}{j} = \prod_{k=1}^{\ell} p_k^{e_k - f_k}, \quad \frac{r}{j'} = \prod_{k=1}^{\ell} p_k^{e_k - g_k}$$

et comme $j \wedge j' = 1$, $f_k \cdot g_k = 0$, donc $\max\{e_k - f_k, e_k - g_k\} = e_k$, ce qui montre que

$$\frac{r}{j} \vee \frac{r}{j'} = r$$

On peut ainsi calculer r, en temps polynomial, à partir de $\frac{j}{r}$ et $\frac{j'}{r}$:
- on connait $\frac{j}{r}$ sous forme d'une fraction $\frac{p}{q}$
- on connait $\frac{j'}{r}$ sous forme d'une fraction $\frac{p'}{q'}$

On calcule

$$\begin{aligned} r &= \frac{q}{p} \vee \frac{q'}{p'} \\ &= \frac{qp'}{pp'} \vee \frac{q'p}{pp'} \\ &= \frac{qp' \vee q'p}{pp'} \\ &= \frac{qp'q'p}{(qp' \wedge q'p)pp'} \\ &= \frac{qq'}{qp' \wedge qp'} \end{aligned}$$

Le calcul de $qp' \wedge qp'$ par l'algorithme d' Euclide prend un temps polynomial (par rapport à n).