ENSEIRB-MATMECA
Option second semestre, 2015/2016

Information Quantique

Examen du 17 Mai 2016

Durée : 2H
Documents autorisés : tous documents autorisés.
Indications : les exercices sont indépendants.
Notation : le barème est indicatif.

Exercice 1 (/10 pts)

Interféromètre de Mach-Zehnder.

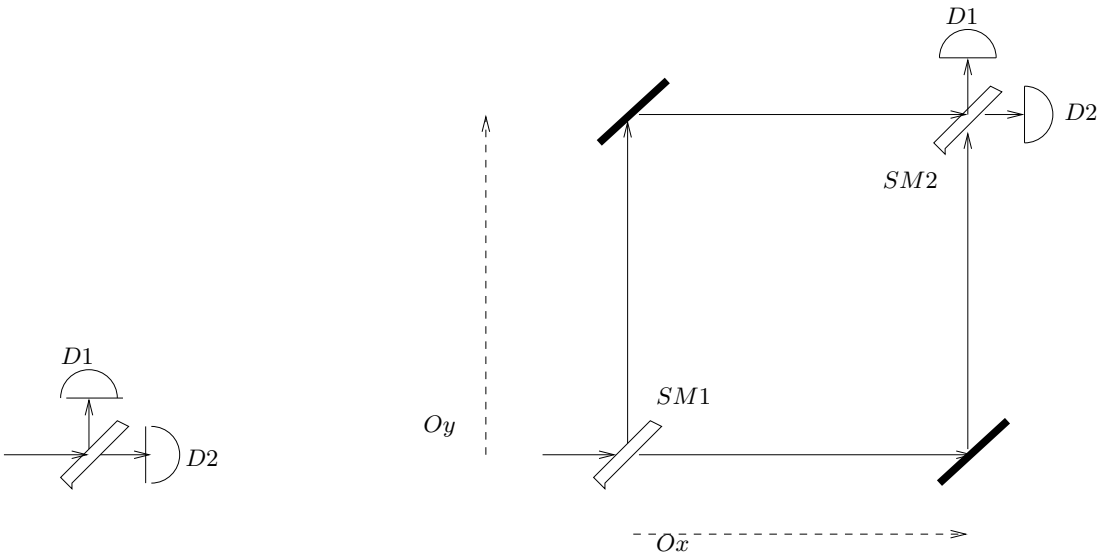

FIGURE 1 – Interféromètre de Mach-Zehnder.

Si on envoie un faisceau lumineux sur une lame semi-réfléchissante, on observe un rayon transmis et un rayon réfléchi chacun d'intensité moitié de celle du rayon incident (figure 1, schéma de gauche). L'interféromètre de Mach-Zehnder (figure 1, schéma de droite) est une succession de deux lames semi-réfléchissantes ($SM1, SM2$) séparées par des miroirs. Le problème est

de déterminer la quantité de lumière arrivant dans les détecteurs D_1 et D_2.
Interprétation quantique.
La lumière est constituée de photons. On associe à la direction de propagation du photon suivant Ox un état quantique $|x\rangle$ et un état quantique $|y\rangle$ à la direction de propagation du photon suivant Oy ; l'action d'une lame semi réfléchissante sur l'état du photon est de le projeter dans un état de superposition

$$\begin{aligned} |x\rangle &\rightarrow \frac{1}{\sqrt{2}}\left[|x\rangle + i\,|y\rangle\right] \\ |y\rangle &\rightarrow \frac{1}{\sqrt{2}}\left[|y\rangle + i\,|x\rangle\right] \end{aligned}$$

tandis que l'action d'un miroir est

$$\begin{aligned} |x\rangle &\rightarrow i\,|y\rangle \\ |y\rangle &\rightarrow i\,|x\rangle \end{aligned}$$

1- Calculer l'état du photon après la première lame ($SM1$), puis après le passage dans le couple de miroirs, puis après la seconde lame ($SM2$).
2- En déduire avec quelle probabilité le photon arrive dans chaque détecteur D_1 et D_2.
Ce phénomène est vu comme une sorte d'interférence du photon avec lui-même (i.e. le photon se trouve, après le passage dans la première lame, dans une superposition de deux états qui interfèrent lorsqu'ils atteignent la deuxième lame).

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 donc 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).
3- Quelles sont maintenant les deux issues possibles de l'expérience ? avec quelles probabilités ?
Supposons que l'on reproduise N fois cette expérience (avec un observateur qui mesure le passage du photon par la gauche ou la droite). Combien de fois, en moyenne, le photon sera-t-il détecté en D_1 ?

Le professeur Cosinus [1] souhaite tirer parti de ce phénomène pour *communiquer*. Il construit pour cela deux montages de Mach-Zehnder, assemblés "tête-bêche" comme sur la figure 2. L'expérience consiste maintenant à en-

1. dont la distraction est légendaire

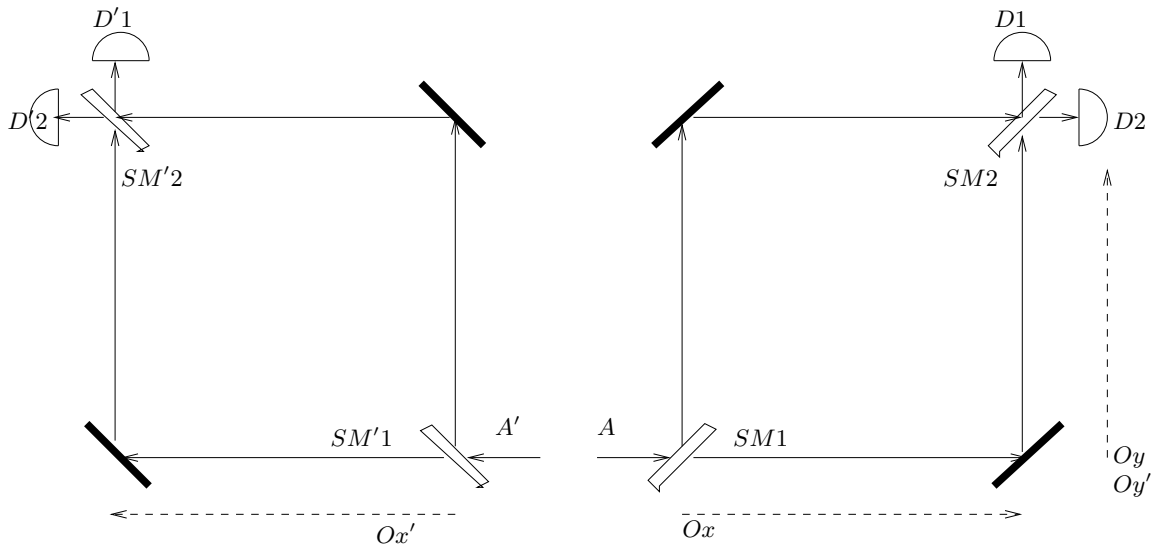

FIGURE 2 – Deux interféromètres de Mach-Zehnder.

voyer deux photons (A, A') ; le photon A est envoyé dans le montage initial (à droite sur la figure), le photon A' dans le montage symétrique (à gauche sur la figure). Le photon A est finalement détecté par D_1, D_2 (comme précédemment) tandis que le photon A' est détecté par D'_1, D'_2.
4- Si les photons (A, A') ont pour état initial $|x\rangle \otimes |x'\rangle$, et si un observateur mesure le photon A en D_1, D_2 , tandisqu'un autre observateur mesure le photon A' en D'_1, D'_2, qu'observent-ils ?

Le professeur Cosinus se dit : si on remplace les deux lames semi-réfléchissantes $SM1, SM'1$ initiales par un système qui prépare les deux photons (A, A') dans l'état *intriqué* $\frac{1}{\sqrt{2}}(|x\rangle \otimes |x'\rangle + |y\rangle \otimes |y'\rangle)$ et si je mesure le photon A juste avant $SM2$ (comme à la Q3), non seulement l'auto-interférence de A cesse, mais, par intrication, celle de A' aussi (voir figure 3) ! Par conséquent, si on répète 100 fois l'expérience, je peux, par mes mesures avant la lame $SM2$, supprimer (ou au contraire permettre) le phénomène d'auto-interférence à la seconde lame. Un observateur (le professeur Sinus) situé en D'_1, D'_2, pourra ainsi savoir si je mesure (ou non). Plus précisément, je peux communiquer avec cet observateur, en procédant comme suit :
- j'initialise toujours les photons dans l'état $\frac{1}{\sqrt{2}}(|x\rangle \otimes |x'\rangle + |y\rangle \otimes |y'\rangle)$ (un automate est réglé pour faire ce travail)

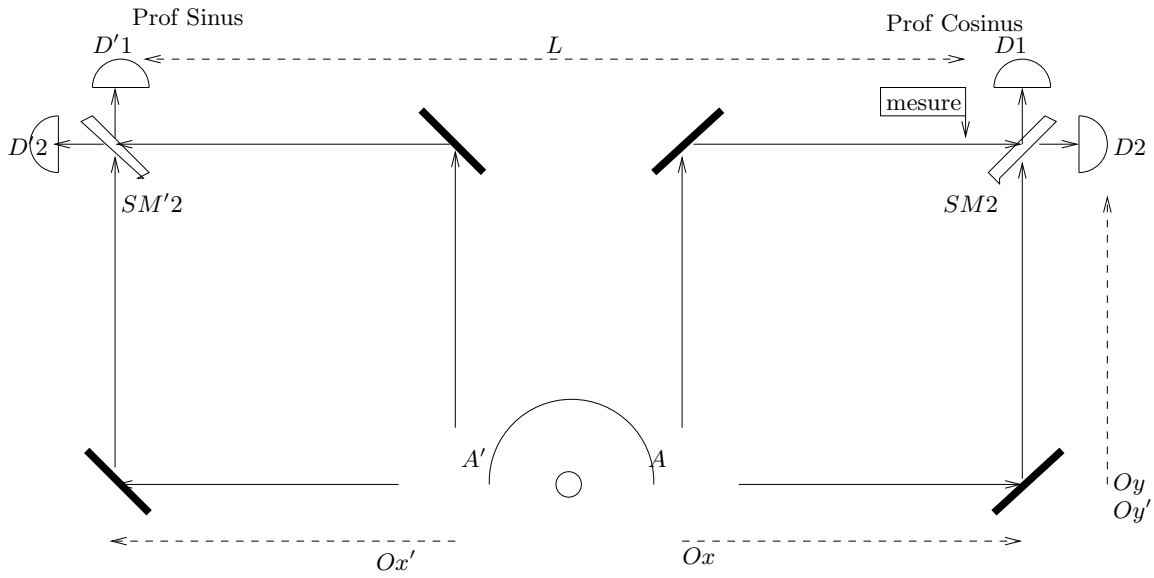

FIGURE 3 – Photons intriqués dans Mach-Zehnder.

- pour transmettre le bit 0 : 100 fois de suite, je laisse les photons (initialisés dans l'état $\frac{1}{\sqrt{2}}(|x\rangle \otimes |x'\rangle + |y\rangle \otimes |y'\rangle)$) suivre leurs trajets, *sans rien mesurer* et mon collègue Sinus mesure le passage de A' dans D'_1 ou D'_2
- pour transmettre le bit 1, 100 fois de suite, *je mesure* le photon A, juste avant la lame $SM2$, et mon collègue Sinus mesure le passage de A' dans D'_1 ou D'_2.

Cosinus se dit que :
si la distance L [entre l'appareil de mesure de Cosinus et les détecteurs D'_1, D'_2] et l'intervalle de temps τ [entre deux envois des couples de photons A, A'] sont tels que

$$100\tau < \frac{L}{2c}$$

alors je parviens à communiquer un bit d'information à une vitesse $> 2c$.
Examinons les idées de Cosinus.
5- Dans son scénario, l'état initial du système (A, A') est $\frac{1}{\sqrt{2}}(|x\rangle \otimes |x'\rangle + |y\rangle \otimes |y'\rangle)$.
Quel est l'état du système (A, A'), après le passage dans le miroir ?
6- 6.1 Quel est l'état du système (A, A'), sans mesure de Cosinus (s'il transmet 0), avant $SM2$? après $SM2$?

6.2 Quel est l'état du système (A, A'), après la mesure de Cosinus (s'il transmet 1) ? avant $SM2$? après $SM2$?
7- Qu'observe le professeur Sinus dans le cas où Cosinus "transmet" 0 ? dans le cas où Cosinus "transmet" 1 ?
8- Cosinus a-t-il réussi à transmettre une information à une vitesse deux fois supérieure à celle de la lumière ?

Exercice 2(/10 pts)

Ordre multiplicatif d'un nombre a modulo N.

Soit N, a deux entiers, $a \in [0, N-1]$. On suppose que a est premier avec N. On se préoccupe de calculer l'*ordre* r de a modulo N c'est-à-dire

$$r := \min\{k \in \mathbb{N} \mid k \geq 1 \text{ et } a^k \equiv 1 \pmod{N}\} \tag{1}$$

Pour tout entier $x \in [0, 2^n - 1]$ on note

$$|x\rangle = |x_1 \dots x_j \dots x_n\rangle$$

le vecteur de $\mathcal{B}^{\otimes n}$ associé à la représentation de x en base 2 i.e. $x = x_1 2^{n-1} + \dots + x_j 2^{n-j} + \dots + 2^0 x_n$ et $\forall j \in [1, n], x_j \in \{0, 1\}$.
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- Rappeler pourquoi U est unitaire.
2- Montrer que, pour tout entier $k \in \mathbb{N}$,

$$U^k = I \Leftrightarrow a^k \equiv 1 \pmod{N}.$$

3- Montrer que le spectre de U est inclus dans $\{e^{\frac{2i\pi j}{r}} \mid 0 \leq j \leq r-1\}$.
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

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

Aide : on se souviendra que

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

5- On pose $|\varphi_j\rangle := D_j(U) \cdot |1\rangle$.
Montrer que $|\varphi_j\rangle \in \mathrm{Ker}(U - \omega_j I)$ et $|\varphi_j\rangle \neq \overrightarrow{0}$.
Que peut-on en déduire sur le spectre de U ?
6- On pose $|\psi_j\rangle := \frac{\omega_j}{\sqrt{r}} |\varphi_j\rangle$.
Montrer que $(|\psi_j\rangle)_{j\in[0,r-1]}$ est une famille orthonormée.
7- Montrer que $\sum_{j=0}^{r-1} |\psi_j\rangle = |1\rangle$.
On a vu en cours un circuit (utilisant l'opérateur U), calculant un opérateur unitaire V sur $2n$ qbits tel que, pour tout vecteur propre $|\psi_j\rangle$

$$V \cdot |0\rangle |\psi_j\rangle = \left|\psi'_j\right\rangle$$

et, lorsqu'on mesure les n premiers q-bits de cet état $\left|\psi'_j\right\rangle$, on obtient un résultat (aléatoire) $y_j \in [0, 2^n - 1]$ tel que

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

8- Appliquons V au vecteur $|0\rangle \otimes |1\rangle \in \mathcal{B}^{\otimes n} \otimes \mathcal{B}^{\otimes n}$ et mesurons les n premiers q-bits de cet état. On obtient un résultat (aléatoire) $y \in [0, 2^n - 1]$. Que peut-on dire sur la loi de y ?
9- On répète deux fois le calcul de la question 8 : on obtient deux valeurs $y, y' \in [0, 2^n - 1]$. Avec quelle probabilité (et quelle méthode) peut-on espérer obtenir à partir de y, y' le nombre r ?
Aide : on admet que la probabilité que deux nombres entiers soient premiers entre eux est $\geq \frac{6}{\pi^2}$.