Traitement Quantique de l'Information **Lundi 24 Janvier 2022**

Examen final - Salle CM1105 - 16h15 à 19h15

Nom: ..... **Prénom:** ..... **Section:** .....

- Vous pouvez répondre aux questions en francais ou en anglais.
- Ecrivez votre nom sur chaque feuille double; rendez la donnée avec votre copie SVP.
- **Une liste de formules trigonométriques utiles se trouve à la fin.**

Problème 1: Interféromètre pour des particules intriquées (25 points).

On considère l'interféromètre de la figure ci-dessous. Deux particules sont émises par la source et l'une se propage vers la gauche alors que l'autre se propage vers la droite. De plus elles sont intriquées: à la sortie de la source les particules de la paire prennent les directions oppos es x, x ou y, y. En d'autres termes l'état quantique émis par la source est de la forme:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|x\rangle_1 \otimes |x\rangle_2 + |y\rangle_1 \otimes |y\rangle_2)$$

où $|x\rangle$, $|y\rangle$ forment une base orthonormée de $\mathbb{C}^2$. Les particules parcourent les bras de l'interféromètre dans les directions x et y. Elles rencontrent les déphaseurs d'angles α, β le long de x, puis les miroirs parfaitement réfléchissants, puis les miroirs semi-transparents, et enfin elles aboutissent dans les détecteurs.

Les déphaseurs sont définis par $D(\theta)|x\rangle = e^{i\theta}|x\rangle$ et $D(\theta)|y\rangle = |y\rangle$ pour $\theta = \alpha, \beta$. Les miroirs parfaitement réfléchissants sont définis par $R|x\rangle = |y\rangle$ et $R|y\rangle = |x\rangle$, et les mirroirs semi-transparents par $S|x\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$, $S|y\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle)$. Ces opérations ont lieu à gauche et à droite et on les notera donc $D_1(\alpha)$, $D_2(\beta)$, R_1, R_2, S_1, S_2.

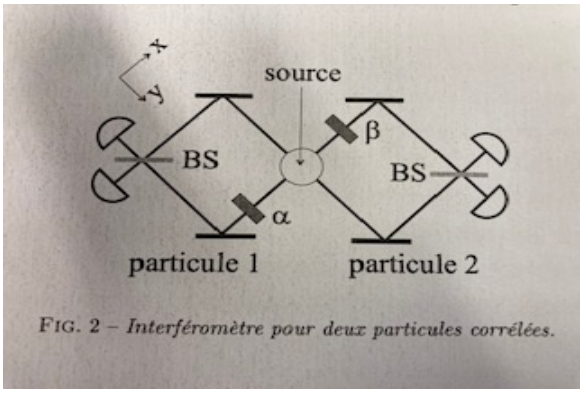

FIG. 2 – *Interféromètre pour deux particules corrélées.*

a) Quel est l'espace d'Hilbert approprié pour décrire le système ? Ecrivez la *matrice unitaire* décrivant l'interféromètre comme un "produit" des matrices définies plus haut.
Indication: il y a deux types de "produits" qui interviennent dans cette expression. On ne

vous demande PAS de calculer ce produit mais juste de l'écrire en spécifiant attentivement les deux types de produits.

b) Calculez maintenant l'état à la sortie de l'interféromètre juste avant les détecteurs. Faites ces calculs en notation de Dirac.

c) Supposons que la source émet une paire dans l'état $|\Psi\rangle$.

- Quels sont tous les états possibles de la paire une fois les particules détectées (c'est à dire après une mesure dans la base $\{|x\rangle, |y\rangle\}$) ?
- Combien de détecteurs cliquent lors de la détection ? Choisissez votre réponse:
  - Un seul.
  - Exactement deux.
  - Ca peut dépendre de α et β: parfois deux ou parfois les quatre.

d) Calculez toutes les probabilités associées aux états possibles obtenus après la mesure.

e) Quelles sont les conditions sur α et β dans $[0, 2\pi]$ pour avoir:

- Les deux particules détectées dans la même direction avec probabilité un.
- Les deux particules détectées dans des directions opposées avec probabilité un.
- Les particules détectées dans toutes les directions avec probabilité uniforme (sortie complèment aléatoire).

Problème 2: Un protocole de génération de one-time pad (25 points).

Dans ce problème nous étudions quelques aspects du protocole de Ekert 1991 pour la génération d'un one-time pad entre deux acteurs distants "Alice" et "Bob".

On rappelle la notation suivante utilisée en cours pour les états (de polarization linéaire p.ex) $|\alpha\rangle$ et $|\alpha_\perp\rangle$ avec ici $\alpha_\perp = \alpha + \frac{\pi}{2}$:

$$|\alpha\rangle = (\cos\alpha)|0\rangle + (\sin\alpha)|1\rangle$$

et

$$|\alpha_\perp\rangle = (\cos\alpha_\perp)|0\rangle + (\sin\alpha_\perp)|1\rangle = (-\sin\alpha)|0\rangle + (\cos\alpha)|1\rangle.$$

Nous supposons qu'Alice et Bob partagent N paires EPR chacune dans l'état de Bell $|B\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Le protocole est constitué des étapes suivantes:

- A chaque instant $k = 1, \ldots, N$ Alice tire au hasard un angle $\alpha_k \in \{-\frac{\pi}{4}, -\frac{\pi}{8}, 0\}$ et fait une mesure de l'observable $A(\alpha_k) = (+1)|\alpha_k\rangle\langle\alpha_k| + (-1)|\alpha_{k,\perp}\rangle\langle\alpha_{k,\perp}|$. Elle enregistre le résultat de la mesure dans la variable aléatoire $a_k \in \{+1, -1\}$.

  Note: on rappelle que l'observable $A(\alpha)$ est mesurée avec un appareil correspondant à la base de mesure $\{|\alpha\rangle, |\alpha_\perp\rangle\}$ et que si l'état après la mesure est $|\alpha\rangle$ (resp. $|\alpha_\perp\rangle$) on enregistre la valeur propre $+1$ (resp. -1).

- Bob fait de même mais pour des angles différents. A chaque instant $k = 1, \ldots, N$ il tire au hasard un angle $\beta_k \in \{-\frac{\pi}{8}, 0, \frac{\pi}{8}\}$ et fait une mesure de l'observable $B(\beta_k) = (+1)|\beta_k\rangle\langle\beta_k| + (-1)|\beta_{k,\perp}\rangle\langle\beta_{k,\perp}|$. Il enregistre le résultat de la mesure dans la variable aléatoire $b_k \in \{+1, -1\}$.

- Jusqu'ici Alice et Bob n'ont pas communiqué. Maintenant, avoir complété leurs mesures, Alice et Bob révèlent sur un canal classique public leurs choix des angles α_k, β_k pour tous les instants k.

- Pour les k tels que $\alpha_k = \beta_k = 0$ ils gardent les bits (a_k, b_k) secrets. Vous montrerez que $a_k = b_k$. Ces bits constituent le one-time pad.

- Alice et Bob effectuent un test de sécurité en calculant la moyenne *empirique* de l'observable

$$S = A(0) \otimes B(\frac{\pi}{8}) + A(0) \otimes B(-\frac{\pi}{8}) - A(-\frac{\pi}{4}) \otimes B(\frac{\pi}{8}) + A(-\frac{\pi}{4}) \otimes B(-\frac{\pi}{8})$$

  Ils déclarent que la communication est sécurisée si cette moyenne empirique est supérieure à $2 + \sigma$ pour un paramètre de sécurité $\sigma > 0$ qui est prédéfini à l'avance.

a) Pour un instant général k calculez les 4 probabilités jointes $\mathbb{P}(a_k = \pm 1, b_k = \pm 1)$. En déduire $\mathbb{P}(a_k = \pm 1)$ et $\mathbb{P}(b_k = \pm 1)$.

b) Montrez que pour k tel que $\alpha_k = \beta_k = 0$ on a $\mathbb{P}(a_k = b_k) = 1$. Ces bits, étant égaux, ils constituent la clé secrète. Quel est la longueur moyenne de cette clé ?

c) On considère l'observable S.

- Quelle est l'expression de sa moyenne *empirique* (c'est à dire obtenue lors de l'expérience) en fonction des bits a_k et b_k ? (on ne demande pas de calcul).

- Quelle est l'expression *théorique* de cette moyenne, c.a.d donnée en fonction de $|B\rangle$ et S par la physique quantique et vue en cours ? (nouveau on ne demande pas de calculs).

- Pourriez vous dire la moyenne théorique vaut et dans quel contexte nous avons vu cette valeur ? (on ne demande pas les calculs).

d) On considère maintenant une attaque simple de la part de Eve. Celle-ci capture les particules destinées à Bob et fait une mesure dans une base choisie au hasard $\{|\theta\rangle, |\theta_\perp\rangle\}$. Quel sont les états possibles de la paire EPR après la mesure de Eve ?

e) Soit γ et γ' deux angles quelconques.

- Calculez $\langle\gamma| \otimes \langle\gamma'|S|\gamma\rangle \otimes |\gamma'\rangle$ (donnez une expression trigonométrique).

- Pour l'attaque ci-dessus de Eve quelles sont les valeurs possibles de (γ, γ') ?

- *Prouvez* que la valeur moyenne théorique de S pour une attaque de Eve (dans le cas simple ci-dessus) est nécessairement ≤ 2. Justifiez en une ou deux phrases le test de sécurité d'Alice et Bob.

Problème 3: Dynamique du spin (25 points).

On considère la dynamique d'un spin dans un champ magnétique dépendant du temps $\vec{B}(t) = (B_1 \cos\omega t, B_1 \sin\omega t, B_0)$. Comme vu en cours, si on se place dans un référentiel tournant (de vitesse angulaire ω) l'hamiltonien du système devient indépendant du temps

$$H = -\frac{\hbar\Delta}{2}\sigma_z - \frac{\hbar\omega_1}{2}\sigma_x$$

où $\Delta = \omega_0 - \omega$ est le paramètre de "detuning" et $\omega_0 \propto B_0$ la fréquence de Larmor et $\omega_1 \propto B_1$ l'intensité de la composante tournante du champ. On travaillera ici exclusivement avec les paramètres Δ et ω_1.

On rappelle l'expression des matrices de Pauli $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. On rappelle aussi l'expression de l'opérateur d'évolution pour un Hamiltonien indépendant du temps

$$U(t) = \exp\left(-\frac{it}{\hbar}H\right)$$

a) Prouvez la formule $e^{i\alpha\hat{n}\cdot\vec{\sigma}} = (\cos\alpha)I + i(\sin\alpha)\hat{n}\cdot\vec{\sigma}$ où $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ et $\hat{n} = (n_x, n_y, n_z)$ est un vecteur unité. Ici $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
Indication: montrez d'abord que $(\hat{n}\cdot\vec{\sigma})^2 = I$.

b) Supposons que le spin soit dans un état initial $|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ à l'instant $t = 0$.

- Calculez l'état au temps t (exprimez le résultat en notation de Dirac).
- Quel est l'état pour $t = t_1 = \frac{\pi}{2\omega_1}$ dans le régime $\Delta \ll \omega_1$ (c.a.d on vous demande la limite de l'état lorsque $\frac{\Delta}{\omega_1} \to 0$).

c) En t_1 on déclenche le champ B_1, c'est à dire qu'on le met à zero $B_1 = 0$, pendant un intervalle de temps $T = \frac{\pi}{\Delta}$. Calculez l'état au temps $t_1 + T$ dans le régime $\Delta \ll \omega_1$ (c.a.d dans la limite $\frac{\Delta}{\omega_1} \to 0$).

d) Finalement au temps $t_1 + T$ on enclenche le champ B_1 à nouveau pendant un intervalle de temps t_1. Calculez maintenant l'état au temps final $t_2 = 2t_1 + T$ toujours pour $\Delta \ll \omega_1$ (c.a.d pour $\frac{\Delta}{\omega_1} \to 0$).

e) Dessinez sur la sphère de Bloch l'état initial et les états trouvés en b), c), d) dans le régime $\Delta \ll \omega_1$.

Note: une suite d'opérations similaires est utilisée dans la méthode de Ramsey pour une mesure précise des fréquences de transitions atomiques dans les horloges atomiques p.ex.

Trigométrie:

- $\cos(a+b) = \cos a \cos b - \sin a \sin b$
- $\sin(a+b) = \cos a \sin b + \sin a \cos b$
- $\cos\big(a+\frac{\pi}{2}\big) = -\sin a$, $\sin\big(a+\frac{\pi}{2}\big) = \cos a$
- $\cos 2a = (\cos a)^2 - (\sin a)^2$, $\sin 2a = 2\sin a \cos a$
- $\cos(-a) = \cos a$, $\sin(-a) = -\sin a$
- $\cos(0) = 1$, $\cos\frac{\pi}{2} = 0$
- $\sin(0) = 0$, $\sin\frac{\pi}{2} = 1$
- $\cos\frac{\pi}{4} = \sin\frac{\pi}{4} = \frac{1}{\sqrt{2}}$
- $\cos a = \frac{1}{2}(e^{ia} + e^{-ia})$, $i\sin a = \frac{1}{2}(e^{ia} - e^{-ia})$
- $e^{ia} = \cos a + i \sin a$
- $e^{ia} = \sum_{k=0}^{+\infty} \frac{(ia)^k}{k!}$
- $\cos a = \sum_{l=0}^{+\infty} \frac{(ia)^{2l}}{(2l)!}$
- $i\sin a = \sum_{l=0}^{+\infty} \frac{(ia)^{2l+1}}{(2l+1)!}$