Série 6
Traitement Quantique de l'Information

Exercice 1 *Relation d'incertitude de Heisenberg*

Le but de cet exercice est de prouver l'inégalité de Heisenberg

$$\Delta A \cdot \Delta B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|.$$

Voir les notes de cours pour la définition de ΔA, ΔB et $[A,B]$. Ici A et B sont hermitiennes. Tout d'abord considérez les obserables de moyenne nulle (pourquoi est elle nulle ?) $A' = A - \langle\psi|A|\psi\rangle$ et $B' = B - \langle\psi|B|\psi\rangle$. Montrez que l'inégalité est equivalente à

$$\Delta A' \cdot \Delta B' \geq \frac{1}{2}|\langle\psi|[A',B']|\psi\rangle|.$$

1. *Première méthode.* Considérez le vecteur $(A + iB)|\psi\rangle$. Montrez que sa norme au carré est un polynome du second degré en λ. Ce polynome doit être positif pour tout λ : pourquoi ? En déduire l'inégalité de Heisenberg.
2. *Deuxième méthode.* Considérez le membre de droite de l'inégalité de Heisenberg. Si vous développez le commutateur, puis utlisez l'inégalité triangulaire, vous obtenez deux termes. Appliquez de manière appropriée l'inégalité de Cauchy-Schwarz pour en déduire l'inégalité de Heisenberg. remarque : en fait la première méthode de preuve est plus satisfaisante car elle "contient" la preuve de l'inégalité de Cauchy-Schwarz.
3. Soit $|\psi\rangle = |\uparrow\rangle$, et $A = \sigma_x$, $B = \sigma_y$. Appliquez l'inégalité de Heisenberg.
4. Cette question est un complément au cours. Considérez l'espace de Hilbert $\mathcal{H} = L^2(\mathbf{R})$ dans l'espace à une dimension spatiale. Les états sont des fonctions d'ondes $\psi(x)$ de carré integrable. L'observable position est l'opérateur de multiplication $\hat{x}$ defini par $(\hat{x}\psi)(x) = x\psi(x)$ et l'observable impulsion (quantité de mouvement) $\hat{p}$ est définie comme $(\hat{p}\psi)(x) = -i\hbar\frac{d}{dx}\psi(x)$. Calculez le commutateur $[\hat{x},\hat{p}]$. Interprétez la relation d'incertitude.

Exercice 2 *Protocole de Bennet 1992*

L'analyse de BB84 montre que le point important du protocole est l'utilisation d'états de qubits non-orthogonaux. Le protocole B92 retient cette caractéristique mais est plus simple à implémenter que BB84. En effet deux états non-orthogonaux sont utilisés au lieu de 4. Voici les phases principales du protocole :

Alice encode. Alice genère une suite binaire aléatoire $e_1, ..., e_N$. Elle envoie à Bob $|A_{e_i}\rangle = |0\rangle$ if $e_i = 0$ and $|A_{e_i}\rangle = H|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$ if $e_i = 1$. Létat du qubit envoyé est donc $H^{e_i}|0\rangle$.

Bob decode. Bob genère une binaire aléatoire $d_1, ..., d_N$ et measure le qubit recu selon la valeur de d_i dans la base Z ou X et obtient un état dans $\{|0\rangle, |1\rangle\}$ ou dans $\{H|0\rangle, H|1\rangle\}$. Il décode le qubit comme $y_i = 0$ si le résultat de la mesure est $|0\rangle$ or $H|0\rangle$ et $y_i = 1$ si le résultat de la mesure est $|1\rangle$ or $H|1\rangle$.

Discussion Publique. Bob annonce sur un canal public ses résultats y_i. Si $e_i = d_i$ on a $y_i = 0$ avec probabilité 1 : prouvez le. Si par contre $e_i \neq d_i$ on a $y_i = 0$ avec probabilité $\frac{1}{2}$ et $y_i = 1$ avec probabilité $\frac{1}{2}$: prouvez le. A partir de cette discussion publique Alice et Bb deduisent que si $y_i = 1$, alors $d_i = 1 - e_i$.

Key generation. Alice et Bob gardent secrets les bits $(e_i, d_i = 1 - e_i)$ pour i tels que $y_i = 1$ et rejettent les autres bits. Expliquez pourquoi cela constitue leur clé secrete. Quelle est la longeur de cette clé. Proposez un test de sécurité qu'ils pourraient faire sur une petite fraction de ces bits.

Attaques de la part d'Eve. Discutez dans le même esprit que dans le cours pourquoi le test de sécurité est violé si Eve capture un photon et essaye une attaque de type "mesure" ou de type "unitaire".