Solution de la série 6
Traitement Quantique de l'Information

Exercice 1 *Heisenberg Uncertainty Principle.*

1. Let $|\phi_\lambda\rangle = (A + i\lambda B)|\psi\rangle$. For $\lambda \in \mathbb{R}$, let us define $f(\lambda) = \langle\psi_\lambda|\,\psi_\lambda\rangle$. It is clear that for any $\lambda \in \mathbb{R}$, $f(\lambda) \geq 0$. We also have

$$\begin{aligned} f(\lambda) &= \langle\psi|\,(A^\dagger - i\lambda^* B^\dagger)(A + i\lambda B)\,|\psi\rangle = \langle\psi|\,(A - i\lambda B)(A + i\lambda B)\,|\psi\rangle \\ &= \langle\psi|\,A^2\,|\psi\rangle + \lambda^2\,\langle\psi|\,B^2\,|\psi\rangle + i\lambda\,\langle\psi|\,(AB - BA)\,|\psi\rangle \\ &= \langle\psi|\,A^2\,|\psi\rangle + \lambda^2\,\langle\psi|\,B^2\,|\psi\rangle + \lambda\,\langle\psi|\,i[A,B]\,|\psi\rangle\,, \end{aligned}$$

where we used the Hermitian property of A and B and the fact that $\lambda \in \mathbb{R}$, thus $\lambda = \lambda^*$. First one can simply check that the operator $i[A,B]$ is a Hermitian operator so the last term $\langle\psi|\,i[A,B]\,|\psi\rangle$ is real-valued so $f(\lambda)$ is real-valued (this was already clear). We see that $f(\lambda)$ is a second order polynomial in $\lambda \in \mathbb{R}$. As it is non-negative for every value of λ, it results that its discriminant must be negative or zero (for a quadratic equation $ax^2 + bx + c = 0$ the discriminant is defined by $\Delta = b^2 - 4ac$). Hence, we get

$$|\,\langle\psi|\,[A,B]\,|\psi\rangle\,|^2 \leq 4\,\langle\psi|\,A^2\,|\psi\rangle\,\langle\psi|\,B^2\,|\psi\rangle\,.$$

As we assumed that the operators have zero mean, $\langle\psi|\,A\,|\psi\rangle = \langle\psi|\,B\,|\psi\rangle = 0$, we obtain that

$$\Delta A\,\Delta B \geq \sqrt{\frac{|\,\langle\psi|\,[A,B]\,|\psi\rangle\,|^2}{4}} = \frac{|\,\langle\psi|\,[A,B]\,|\psi\rangle\,|}{2}$$

2. This time we will use Cauchy-Schwartz inequality that $|\,\langle a|\,b\rangle\,|^2 \leq \langle a|\,a\rangle\,\langle b|\,b\rangle$ for any vector a and b in any Hilbert space. We also use the following inequality that for any two complex numbers x and y, $|x-y|^2 \leq 2(|x|^2 + |y|^2)$ which one can simply prove.

$$\begin{aligned} |\,\langle\psi|\,[A,B]\,|\psi\rangle\,|^2 &= |\,\langle\psi|\,AB\,|\psi\rangle - \langle\psi|\,BA\,|\psi\rangle\,|^2 \overset{(a)}{\leq} 2(|\,\langle\psi|\,AB\,|\psi\rangle\,|^2 + |\,\langle\psi|\,BA\,|\psi\rangle\,|^2) \\ &\overset{(b)}{\leq} 2(\langle\psi|\,AA^\dagger\,|\psi\rangle\,\langle\psi|\,B^\dagger B\,|\psi\rangle + \langle\psi|\,BB^\dagger\,|\psi\rangle\,\langle\psi|\,A^\dagger A\,|\psi\rangle) \\ &\overset{(c)}{=} 4\,\langle\psi|\,A^2\,|\psi\rangle\,\langle\psi|\,B^2\,|\psi\rangle = 4(\Delta A)^2(\Delta B)^2, \end{aligned}$$

where (a) follows from the inequality for complex numbers just mentioned, (b) follows by applying the Cauchy-Schwartz inequality and (c) follows from the Hermitian property of A and B.

3. For $\psi = |\uparrow\rangle$ and $A = \sigma_x$ and $B = \sigma_y$, we have

$$\begin{aligned}
\bar{A} &= \langle\psi| A |\psi\rangle = (1 \;\; 0) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0, \\
\bar{A^2} &= \langle\psi| A^2 |\psi\rangle = (1 \;\; 0) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1, \\
\bar{B} &= \langle\psi| B |\psi\rangle = (1 \;\; 0) \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0, \\
\bar{B^2} &= \langle\psi| B^2 |\psi\rangle = (1 \;\; 0) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1,
\end{aligned}$$

where for an operator C, $\bar{C}$ denotes the average of the operator in state $|\psi\rangle$. Therefore, we get

$$(\Delta A)^2 = \langle\psi| A^2 |\psi\rangle - (\langle\psi| A |\psi\rangle)^2 = 1, (\Delta B)^2 = \langle\psi| B^2 |\psi\rangle - (\langle\psi| B |\psi\rangle)^2 = 1.$$

We also know that the Pauli matrices satisfy the identity $[\sigma_x, \sigma_y] = 2i\sigma_z$. Thus, we have

$$\langle\psi| [A, B] |\psi\rangle = 2i(1 \;\; 0) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 2i,$$

which satisfies the uncertainty principle

$$(\Delta A)^2(\Delta B)^2 = 1 \geq \frac{|2i|^2}{4} = \frac{|\langle\psi| [A, B] |\psi\rangle|^2}{4}.$$

In particular, in this case the uncertainty inequality turns out to be an equality.

4. In this exercise, the state of a particle is represented by a function of coordinate variable $\psi(x)$. We also know how $\hat{x}$ and $\hat{p}$ operators transform this state function. To find the commutator of $\hat{x}$ and $\hat{p}$, we take an arbitrary state function $\phi(x)$ and investigate how $[\hat{x}, \hat{p}]$ operates on it. Specifically we have

$$\begin{aligned}
&(\hat{p}\hat{x})\phi(x) = \hat{p}(\hat{x}\phi(x)) = \hat{p}(x\phi(x)) = -i\hbar\frac{d}{dx}(x\phi(x)) = -i\hbar(\phi(x) + x\frac{d}{dx}\phi(x)), \\
&(\hat{x}\hat{p})\phi(x) = \hat{x}(-i\hbar\frac{d}{dx}\phi(x)) = -i\hbar x\frac{d}{dx}\phi(x),
\end{aligned}$$

which implies that $[\hat{x}, \hat{p}]\phi(x) = i\hbar\phi(x)$. As ϕ was an arbitrary function, it results that $[\hat{x}, \hat{p}] = i\hbar$.

Exercice 2 *Bennett 1992 Protocol.*

Key Generation : From the explanation, it is clear that when $d_i = e_i$, Bob measures the qubit in the same basis that they are transmitted, i.e. the transmitted qbit state is $|0\rangle$ and the measurement is done in Z-basis which gives $|0\rangle$ with probability 1. A similar argument holds for $H|0\rangle$. Thus when $d_i = e_i$ we certainly have $y_i = 0$. In other words $\mathbb{P}(y_i = 0|d_i = e_i) = 1$ and $\mathbb{P}(y_i = 1|d_i = e_i) = 0$. However, when $d_i \neq e_i$ then for example the transmitted state is $|\psi\rangle = H|0\rangle$ but the measurement is done in the Z-basis which results in $|0\rangle$ or $|1\rangle$ with equal probability because $|\langle 0|\,\psi\rangle|^2 = |\langle 1|\,\psi\rangle|^2 = (1/\sqrt{2})^2 = 1/2$. In other words $\mathbb{P}(y_i = 0|d_i \neq e_i) = \frac{1}{2}$ and $\mathbb{P}(y_i = 1|d_i \neq e_i) = \frac{1}{2}$.

We observe that $y_i = 1$ only when $d_i \neq e_i$. The secret key is then generated as folllows : Alice and Bob reveal the y_i's and keep the $e_i = 1 - d_i$ such that $y_i = 1$ as a secret key. The other e_i and d_i are discarded. Indeed if $y_i = 1$ the Alice and Bob know that $e_i = 1 - d_i$ for sure. This can be proved from the Bayes rule :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\mathbb{P}(y_i = 1|e_i = 1 - d_i)\mathbb{P}(e_i = 1 - d_i)}{\mathbb{P}(y_i = 1)} = \frac{\frac{1}{2} \times \frac{1}{2}}{\frac{1}{4}} = 1$$

In the last equalirty we used

$$\begin{aligned}\mathbb{P}(y_i = 1) &= \mathbb{P}(y_i = 1|e_i = d_i)\mathbb{P}(e_i = d_i) + \mathbb{P}(y_i = 1|e_i \neq d_i)\mathbb{P}(e_i \neq d_i)\\ &= 0 \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}.\end{aligned}$$

Here we have assumed that $\mathbb{P}(e_i \neq d_i) = \mathbb{P}(e_i = d_i) = \frac{1}{2}$.

The length of the resulting secret key is around $N\,\mathbb{P}(y_i = 1) = \frac{N}{4}$, a quarter of the length of the main sequence.

Security Check : Alice and Bob can do a security check by exchanging a small fraction of the secure bits via public channel. If the test is successful they keep the rest of the common substring secure : thus they have succeeded in generating a common secure string. If there is no attack from Eve's side and the transmission channel is perfect, then as we explained we have $e_i = 1 - d_i$ whenever $y_i = 1$. The test is :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = 1.$$

Eve's Attack : Here we discuss only the measurement attack. Alice sends the states $H^{e_i}|0\rangle$ through the optic fiber. Suppose Eve captures a photon and makes a measurement in the Z or the X basis. If she chooses the Z basis she finds the result of the measurement $|0\rangle$ or $|1\rangle$. If she finds $|0\rangle$ she sends this state to Bob. If she finds $|1\rangle$ she deduces that certainly Bob did not send the state $|0\rangle$, and that he must have sent the state $H|0\rangle$. She sends $H|0\rangle$ to Bob. If Eve chooses the X basis she finds the result of the measurement $H|0\rangle$ or $H|1\rangle$. If she finds $H|0\rangle$ she sends this state to Bob. If she finds $H|1\rangle$ she deduces that certainly Bob did not send the state $H|0\rangle$, and that he must have sent the state $|0\rangle$. She sends $|0\rangle$ to Bob. Let $E_i = 0, 1$ denote the choice of Z or X basis for Eve.

Note that we could devise other startegies for Eve but this will not help. If you wish you can devise your own strategy and see how the security criterion is affceted. Here we stick to the above strategy for Eve. Summarizing, we see that Bob receives the states $H^{e_i + E_i}|0\rangle$.

Now Bob decodes and finds the states $H^{d_i}|y_i\rangle$ ($d_i = 0, 1$ according to the basis chosen). From the measurement postulate

$$\mathbb{P}(y_i|e_i, d_i, E_i) = |\langle y_i|H^{e_i + d_i + E_i}|0\rangle|^2$$

In particular given $e_i = 1 - d_i$ we have

$$\mathbb{P}(y_i = 1|e_i = 1 - d_i, E_i) = |\langle y_i|H^{1 + E_i}|0\rangle|^2$$

Thus

$$\begin{aligned}\mathbb{P}(y_i = 1|e_i = 1 - d_i) &= |\langle 1|H|0\rangle|^2 p(E_i = 0) + |\langle 1|H^2|0\rangle|^2 \mathbb{P}(E_i = 1)\\ &= \frac{1}{2}\mathbb{P}(E_i = 0)\end{aligned}$$

Now let us look at the security criterion. By Bayes rule :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\mathbb{P}(y_i = 1|e_i = 1 - d_i)\mathbb{P}(e_i = 1 - d_i)}{\mathbb{P}(y_i = 1)}$$

For the denominator we use (we asume that Eve's choice of E_i is independent of Alice's and Bob's choices of e_i and d_i)

$$\begin{aligned}\mathbb{P}(y_i = 1) &= \sum_{E_i=0,1} \mathbb{P}(y_i = 1|e_i \neq d_i, E_i)\mathbb{P}(e_i \neq d_i, E_i) + \sum_{E_i=0,1} \mathbb{P}(y_i = 1|e_i = d_i, E_i)\mathbb{P}(e_i = d_i, E_i = 1)\\ &= \sum_{E_i=0,1} |\langle 1|H^{1+E_i}|0\rangle|^2 \mathbb{P}(E_i) + \sum_{E_i=0,1} |\langle 1|H^{2+E_i}|0\rangle|^2 \mathbb{P}(E_i)\\ &= |\langle 1|H|0\rangle|^2 \mathbb{P}(E_i = 0) + |\langle 1|H|0\rangle|^2 \mathbb{P}(E_i = 1)\\ &= \frac{1}{2}\end{aligned}$$

For the numerator,

$$\mathbb{P}(y_i = 1|e_i = 1 - d_i) = \sum_{E_i=0,1} |\langle 1|H^{1+E_i}|0\rangle|^2 \mathbb{P}(E_i) = \frac{1}{2}\mathbb{P}(E_i = 0)$$

Putting these results alltogether we obtain :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\frac{1}{2}\mathbb{P}(E_i = 0)\mathbb{P}(e_i = 1 - d_i)}{\frac{1}{2}} = \mathbb{P}(E_i = 0)\mathbb{P}(e_i = 1 - d_i)$$

Supposing that $\mathbb{P}(e_i \neq d_i) = \frac{1}{2}$ we see that $\mathbb{P}(e_i = 1 - d_i|y_i = 1) \leq \frac{1}{2}$ whatever is Eve's strategy for the choice of measurement basis $E_i = 0, 1$.