Quantum Computing - Final

Kishlaya Jaiswal

December 24, 2020

Exercise 1

Suppose $\rho = p\left|0\right\rangle\left\langle 0\right| + (1-p)\frac{(|0\rangle+|1\rangle)(\langle 0|+\langle 1|)}{2}$. Evaluate $S(\rho)$ and compare the value with $H(p)$.

Solution. In the basis $\{|0\rangle, |1\rangle\}$, $\rho = \frac{1}{2}\begin{pmatrix} 1+p & 1-p \\ 1-p & 1-p \end{pmatrix}$ and its eigenvalues are $\lambda(p) = \frac{1}{2}\left(1 - \sqrt{2p^2 - 2p + 1}\right)$ and $1 - \lambda(p)$. Therefore,

$$S(\rho) = H(\lambda) = -\lambda \log \lambda - (1-\lambda)\log(1-\lambda)$$

whereas

$$H(p) = -p\log p - (1-p)\log(1-p)$$

Claim $\forall 0 \leq p \leq 1$, $\lambda(p) \leq p$

Proof. Since $\lambda(0) = 0$ and $\lambda(1) = 0$, we only need to check for $0 < p < 1$.
Consider the quadratic $f(x) = x^2 - (2p-1)x + \frac{p(p-1)}{2}$. Since $f(0) = \frac{p(p-1)}{2} < 0$, one root is greater than 0 and the other root is less than 0. Roots of $f(x)$ are $\frac{2p-1\pm\sqrt{2p^2-2p+1}}{2}$, so we get that $\frac{2p-1+\sqrt{2p^2-2p+1}}{2} > 0 \implies p > \lambda(p)$ □

Furthermore, since the other root of $f(x)$ is $\frac{2p-1-\sqrt{2p^2-2p+1}}{2} < 0 \implies p < 1 - \lambda(p)$, $\forall 0 < p < 1$.

Finally, since $H(p)$ is strictly increasing in $[0, 1/2]$, $H(p) \geq H(\lambda)$. For $[1/2, 1]$ since $H(p)$ is strictly decreasing in this interval $H(p) \geq H(1-\lambda) = H(\lambda)$

Therefore, we get $S(\rho) \leq H(p)$ with equality only at $p = 0, 1$.

■

Exercise 2

Suppose $|AB\rangle$ is a pure state shared between Alice and Bob. Show that $|AB\rangle$ is entangled iff $S(B \mid A) < 0$

Solution. Because $|AB\rangle$ is a pure state $S(A, B) = 0$. Furthermore, since $S(B \mid A) = S(A, B) - S(A)$, we get

$$S(B \mid A) < 0 \iff S(A) > 0$$

Since $|AB\rangle$ is a pure state, we use Schmidt decomposition, that is we can find bases $\{|u_i\rangle_A\}$ and $\{|v_j\rangle_B\}$ such that $|AB\rangle = \sum_{i=1}^{n} \lambda_i |u_i\rangle_A \otimes |v_i\rangle_B$, where λ_i are positive reals and $\sum \lambda_i^2 = 1$.

So $\rho_{AB} = \sum_{i,j} \lambda_i \lambda_j |u_i\rangle \langle u_j| \otimes |v_i\rangle \langle v_j|$ and therefore,

$$\begin{aligned}
\rho_A &= \mathrm{Tr}_B(\rho_{AB}) \\
&= \mathrm{Tr}_B \left(\sum_{1 \le i,j \le n} \lambda_i \lambda_j |u_i\rangle \langle u_j| \otimes |v_i\rangle \langle v_j| \right) \\
&= \sum_{1 \le i,j \le n} \lambda_i \lambda_j \, \mathrm{Tr}_B \left(|u_i\rangle \langle u_j| \otimes |v_i\rangle \langle v_j| \right) \\
&= \sum_{1 \le i,j \le n} \lambda_i \lambda_j |u_i\rangle \langle u_j| \langle v_j \mid v_i\rangle \qquad \text{(homework 3 exercise 2)}
\end{aligned}$$

Thus $\rho_A = \sum \lambda_i^2 |u_i\rangle \langle u_i| \implies S(A) = -\sum \lambda_i^2 \log \lambda_i^2$. So $S(A) \ge 0$.

Suppose $|AB\rangle$ is entangled, then there exist i, j such that $0 < \lambda_i, \lambda_j < 1$. So $S(A) \ge -\lambda_i^2 \log \lambda_i^2 - \lambda_j^2 \log \lambda_j^2 > 0$

Conversely, suppose $|AB\rangle$ is not entangled, then there exists an i such that $|AB\rangle = |u_i\rangle_A \otimes |v_i\rangle_B$. So A is a pure state and hence $S(A) = 0$.

■

Exercise 3(i)

Show that $H(X, Y \mid Z) \ge H(X \mid Z)$

Solution. Note that $H(X, Y \mid Z) \ge H(X \mid Z) \iff H(X, Y, Z) \ge H(X, Z)$.

$$\begin{aligned}
H(X,Y,Z) &= -\sum_{x,y,z} p(x,y,z) \log p(x,y,z) \\
&= -\sum_{x,y,z} p(x,y,z) \log p(y \mid x,z) p(x,z) \\
&= -\sum_{x,y,z} p(x,y,z) \log p(y \mid x,z) - \sum_{x,y,z} p(x,y,z) \log p(x,z) \\
&= -\sum_{x,y,z} p(x,y,z) \log p(y \mid x,z) - \sum_{x,z} \left(\sum_{y} p(x,y,z) \right) \log p(x,z) \\
&= \sum_{x,y,z} p(x,y,z)(-\log p(y \mid x,z)) + H(X,Z)
\end{aligned}$$

Since $(-\log p(y \mid x,z)) \ge 0 \implies \sum_{x,y,z} p(x,y,z)(-\log p(y \mid x,z)) \ge 0$. Therefore, $H(X,Y,Z) \ge H(X,Z)$

■

Exercise 3(ii)

Show that it is not always the case that $S(A, B \mid C) \ge S(A \mid C)$

Solution. Consider $|ABC\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$. So $\rho_{ABC} = \frac{1}{2} \left(|000\rangle \langle 000| + |000\rangle \langle 111| + |111\rangle \langle 000| + |111\rangle \langle 111| \right)$
Since $|ABC\rangle$ is a pure state, $S(A, B, C) = S(\rho_{ABC}) = 0$

Tracing out B we get: $\rho_{AC} = \frac{1}{2} \left(|00\rangle \langle 00| + |11\rangle \langle 11| \right) = \frac{1}{2} I \implies$ eigenvalues of ρ_{AC} are $\frac{1}{2}, \frac{1}{2}$. Hence $S(A, C) = 1$

Therefore, $S(A, B, C) < S(A, C) \implies S(A, B \mid C) < S(A \mid C)$ as desired.

■

Exercise 3(iii)

Prove or disprove $S(A, B \mid C) \geq S(A \mid C) - S(B \mid C)$

Solution. Suppose it was indeed true that for any composite system A, B, C, we had $S(A, B \mid C) \geq S(A \mid C) - S(B \mid C)$ which implies $S(A, B, C) - S(C) \geq S(A, C) - S(B, C)$. Now use strong subadditivity to get $S(A, B, C) \leq S(A, C) + S(B, C) - S(C)$. Together it implies

$$S(C) + S(A, C) - S(B, C) \leq S(A, C) + S(B, C) - S(C) \implies S(B \mid C) \geq 0$$

which we know is incorrect.

To give a concrete counterexample, consider $|ABC\rangle = |0\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

- $S(A, B, C) = 0$ as A, B, C are in a pure state
- $\rho_{AC} = \frac{1}{2}(|00\rangle\langle 00| + |01\rangle\langle 01|) \implies S(A, C) = 1$
- $\rho_{BC} = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) \implies S(B, C) = 0$ as B, C is in a pure state
- $\rho_C = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \implies S(C) = 1$

Setting these values in the inequality $S(A, B, C) - S(C) \geq S(A, C) - S(B, C)$, we get $-1 \geq 1$ which is a contradiction.

■

Exercise 3(iv)

Show that $S(A, B) \geq S(A \mid C) - S(B \mid C)$

Solution. $S(A, B) \geq S(A \mid C) - S(B \mid C) \iff S(A, B) \geq S(A, C) - S(B, C) \iff S(A, C) \leq S(A, B) + S(B, C)$

We can find an environment R such that the composite system A, B, C, R is in a pure state.

- Tracing out A, B, C and R gives us same entropy, that is $S(R) = S(A, B, C)$

  Proof. Using Schmidt decomposition, we can write $|ABCR\rangle = \sum_i \lambda_i |u_i\rangle_{ABC} \otimes |v_i\rangle_R$. Hence $\rho_{ABCR} = \sum_{ij} \lambda_i \lambda_j |u_i\rangle_{ABC} \langle u_j|_{ABC} \otimes |v_i\rangle_R \langle v_j|_R$.
  Thus, $\rho_{ABC} = \mathrm{Tr}_R(\rho_{ABCR}) = \sum_i \lambda_i^2 |u_i\rangle_{ABC} \langle u_i|_{ABC}$. Similarly, $\rho_R = \mathrm{Tr}_{ABC}(\rho_{ABCR}) = \sum_i \lambda_i^2 |v_i\rangle_R \langle v_i|_R$
  In both the cases, $S(A, B, C) = S(R) = -\sum \lambda_i^2 \log \lambda_i^2$ □

- Tracing out A, C and B, R gives us same entropy, that is $S(B, R) = S(A, C)$

  Proof. Using Schmidt decomposition, we can write $|ACBR\rangle = \sum_i \mu_i |x_i\rangle_{AC} \otimes |y_i\rangle_{BR}$. Hence $\rho_{ACBR} = \sum_{ij} \mu_i \mu_j |x_i\rangle_{AC} \langle x_j|_{AC} \otimes |y_i\rangle_{BR} \langle y_j|_{BR}$.
  Thus, $\rho_{AC} = \mathrm{Tr}_{BR}(\rho_{ACBR}) = \sum_i \mu_i^2 |x_i\rangle_{AC} \langle x_i|_{AC}$. Similarly, $\rho_{BR} = \mathrm{Tr}_{AC}(\rho_{ACBR}) = \sum_i \mu_i^2 |y_i\rangle_{BR} \langle y_i|_{BR}$
  In both the cases, $S(A, C) = S(B, R) = -\sum \mu_i^2 \log \mu_i^2$ □

Now using strong subadditivity we have: $S(A, B, C) + S(B) \leq S(A, B) + S(B, C) \implies S(R) + S(B) \leq S(A, B) + S(B, C)$.
But $S(B) + S(R) \geq S(B, R) = S(A, C)$ using subadditivity. Finally,we get $S(A, C) \leq S(A, B) + S(B, C)$ as desired.

■

Exercise 4

Suppose $f : \mathbb{R} \to \mathbb{R}$ is a convex differentiable function. For Hermitian operators A, B show that

$$\mathrm{Tr}(f(A) - f(B)) \geq \mathrm{Tr}((A - B)f'(B))$$

Solution. Let $f : \mathbb{R} \to \mathbb{R}$ be a convex differentiable function and A, B be two $n \times n$ Hermitian matrices. So using spectral theorem, we can find a eigenbasis $\{|u_i\rangle\}$ for $A = \sum \alpha_i |u_i\rangle \langle u_i|$ and an eigenbasis $\{|v_i\rangle\}$ for $B = \sum \beta_i |v_i\rangle \langle v_i|$ such that $\alpha_i, \beta_i \in \mathbb{R}$, $\forall i$.
Then $f(A) = \sum f(\alpha_i) |u_i\rangle \langle u_i|$ and $f(B) = \sum f(\beta_i) |v_i\rangle \langle v_i|$

$$\begin{aligned}
\mathrm{Tr}\left(f(A)\right) &= \sum_i \langle u_i| f(A) |u_i\rangle = \sum_i f(\alpha_i) \\
\mathrm{Tr}\left(f(B)\right) &= \sum_i \langle u_i| f(B) |u_i\rangle = \sum_i \sum_j f(\beta_j) P_{ij}
\end{aligned}$$

where $P_{ij} = \langle u_i \mid v_j\rangle \langle v_j \mid u_i\rangle$. Note that, $P_{ij} = \left|\langle u_i \mid v_j\rangle\right|^2 \geq 0$. Also since $\sum_j P_{ij} = \sum_j \langle v_j \mid u_i\rangle \langle u_i \mid v_j\rangle = 1$, we can re-write $\mathrm{Tr}(f(A)) = \sum_{i,j} f(\alpha_i) P_{ij}$. Thus, we get:

$$\mathrm{Tr}(f(A) - f(B)) = \sum_{i,j} (f(\alpha_i) - f(\beta_j)) P_{ij}$$

Now we state (and prove) a fact about convex differentiable functions.

Lemma. *Let $f : \mathbb{R} \to \mathbb{R}$ be a convex differentiable function then for any two distinct points $x, y \in \mathbb{R}$,*

$$f(x) - f(y) \geq (x - y)f'(y)$$

Proof. Using convexity, we know that for $0 < t < 1$, $f(tx + (1-t)y) \leq tf(x) + (1-t)f(y)$. We re-arrange to get: $f(y + t(x - y)) \leq f(y) + t(f(x) - f(y))$

$$\begin{aligned}
&\implies \frac{f(y + t(x-y)) - f(y)}{t(x-y)} \leq \frac{f(x) - f(y)}{x - y} \quad \text{if } x > y \\
&\implies -\frac{f(y) - f(y - t(y-x))}{t(y-x)} \leq \frac{f(x) - f(y)}{y - x} \quad \text{if } x < y
\end{aligned}$$

This being true for all $t > 0$, we take limit $t \to 0$ to get $(x - y)f'(y) \leq f(x) - f(y)$ □

Therefore, we have $\mathrm{Tr}(f(A) - f(B)) \geq \sum_{i,j} (\alpha_i - \beta_j) f'(\beta_j) P_{ij}$. But we can see this is equal to $\mathrm{Tr}((A - B)f'(B))$ as follows:

$$\begin{aligned}
\mathrm{Tr}(Af'(B)) &= \sum_i \langle u_i| Af'(B) |u_i\rangle \\
&= \sum_i \langle u_i| A \left(\sum_k |u_k\rangle \langle u_k| \right) f'(B) |u_i\rangle \\
&= \sum_i \alpha_i \langle u_i| f'(B) |u_i\rangle \\
&= \sum_{i,j} \alpha_i f'(\beta_j) P_{ij}
\end{aligned}$$

$$
\begin{aligned}
\operatorname{Tr}(Bf'(B)) &= \sum_i \langle u_i| Bf'(B) |u_i\rangle \\
&= \sum_i \langle u_i| \left(\sum_j \beta_j f'(\beta_j) |v_j\rangle \langle v_j| \right) |u_i\rangle \\
&= \sum_{i,j} \beta_j f'(\beta_j) P_{ij}
\end{aligned}
$$

Thus, $\operatorname{Tr}(f(A) - f(B)) \geq \operatorname{Tr}((A - B)f'(B))$ ■

Exercise 5

Give a detailed proof of quantum operations never increase mutual information

Solution. Given a composite system ρ_{AB}, the action of a quantum operation $\mathcal{E}$ on the system B is defined as:

$$
\mathcal{E}(\rho_{AB}) = \operatorname{Tr}_C \Big((I_A \otimes U_{BC})(\rho_{AB} \otimes \rho_C)(I_A \otimes U_{BC}^\dagger) \Big)
$$

where C is the environment in consideration which the system B interacts with. We break this operation in three steps for our convenience of entropy calculations.

1. Introduce the environment ρ_C so that the resulting state is $\rho_{ABC} = \rho_{AB} \otimes \rho_C$

$$
S(A, B, C) = S(\rho_{ABC}) = S(\rho_{AB} \otimes \rho_C) = S(\rho_{AB}) + S(\rho_C) = S(A, B) + S(C)
$$

$$
\begin{aligned}
\rho_{BC} &= \operatorname{Tr}_A(\rho_{ABC}) \\
&= \sum_i (\langle i|_A \otimes I_{BC}) \rho_{AB} \otimes \rho_C (|i\rangle_A \otimes I_{BC}) \\
&= \sum_i (\langle i|_A \otimes I_B \otimes I_C) \rho_{AB} \otimes \rho_C (|i\rangle_A \otimes I_B \otimes I_C) \\
&= \left(\sum_i (\langle i|_A \otimes I_B) \rho_{AB} (|i\rangle_A \otimes I_B) \right) \otimes \rho_C \\
&= \operatorname{Tr}_A(\rho_{AB}) \otimes \rho_C \\
&= \rho_B \otimes \rho_C
\end{aligned}
$$

$$
\implies S(B, C) = S(\rho_{BC}) = S(\rho_B \otimes \rho_C) = S(\rho_B) + S(\rho_C) = S(B) + S(C)
$$

Therefore, $S(A : B, C) = S(A : B)$

2. Apply the Unitary transformation $I_A \otimes U_{BC}$ on the system and so that the resulting state is $(I_A \otimes U_{BC})\rho_{ABC}(I_A \otimes U_{BC}^\dagger)$

We first state and prove a simple lemma which says that unitary transformations do not change entropy.

Lemma. *Let ρ be a density matrix and U be a unitary evolution acting on ρ, then $S(\rho) = S(U\rho U^\dagger)$*

Proof. Let the spectral decomposition of ρ be $\sum_i \lambda_i |\phi_i\rangle \langle\phi_i|$. Then

$$U\rho U^\dagger = \sum_i \lambda_i U |\phi_i\rangle \langle\phi_i| U^\dagger = \sum_i \lambda_i |\psi_i\rangle \langle\psi_i|$$

(where $|\psi_i\rangle = U|\phi_i\rangle$) is the spectral decomposition of $U\rho U^\dagger$ because $\langle\psi_i \mid \psi_j\rangle = \langle\phi_i| U^\dagger U |\phi_j\rangle = 0$ for $i \neq j$, otherwise it is equal to 1. □

So the state ρ_{ABC} now transforms to $\rho_{A'B'C'} = (I_A \otimes U_{BC})\rho_{ABC}(I_A \otimes U_{BC}^\dagger)$. By above lemma, $S(\rho_{ABC}) = S(\rho_{A'B'C'}) \implies S(A,B,C) = S(A',B',C')$. Now we have:

$$\begin{aligned}
\rho_{A'} &= \mathrm{Tr}_{B'C'}(\rho_{A'B'C'}) \\
&= \mathrm{Tr}_{BC}\left((I_A \otimes U_{BC})\rho_{ABC}(I_A \otimes U_{BC}^\dagger)\right) \\
&= \sum_i (I_A \otimes \langle i|_{BC})(I_A \otimes U_{BC})\rho_{ABC}(I_A \otimes U_{BC}^\dagger)(I_A \otimes |i\rangle_{BC}) \\
&= \sum_i (I_A \otimes \langle i|_{BC} U_{BC})\rho_{ABC}(I_A \otimes U_{BC}^\dagger |i\rangle_{BC}) \\
&= \sum_{i'} (I_A \otimes \langle i'|_{BC})\rho_{ABC}(I_A \otimes |i'\rangle_{BC}) \\
&= \mathrm{Tr}_{BC}(\rho_{ABC}) \\
&= \rho_A
\end{aligned}$$

where $|i'\rangle_{BC} = U_{BC}^\dagger |i\rangle_{BC}$ is another orthonormal basis for BC as $U^\dagger$ is a unitary matrix.

$$\begin{aligned}
\rho_{B'C'} &= \mathrm{Tr}_{A'}(\rho_{A'B'C}) \\
&= \mathrm{Tr}_{A}\left((I_A \otimes U_{BC})\rho_{ABC}(I_A \otimes U_{BC}^\dagger)\right) \\
&= \sum_i (\langle i|_A \otimes I_{BC})(I_A \otimes U_{BC})\rho_{ABC}(I_A \otimes U_{BC}^\dagger)(|i\rangle_A \otimes I_{BC}) \\
&= \sum_i (I_A \otimes U_{BC})(\langle i|_A \otimes I_{BC})\rho_{ABC}(|i\rangle_A \otimes I_{BC})(I_A \otimes U_{BC}^\dagger) \\
&= (I_A \otimes U_{BC})\,\mathrm{Tr}_A\,(\rho_{ABC})\,(I_A \otimes U_{BC}^\dagger) \\
&= (I_A \otimes U_{BC})\rho_{BC}(I_A \otimes U_{BC}^\dagger)
\end{aligned}$$

Again using the above lemma, $S(\rho_{BC}) = S(\rho_{B'C'})$.

Putting it all together, we have $S(A) = S(A')$, $S(B,C) = S(B',C')$ and $S(A,B,C) = S(A',B',C')$

$$\implies S(A:B,C) = S(A':B',C')$$

3. Finally trace out the environment C' to get the resulting state.
   We get $S(A':B') = S(A') + S(B') - S(A',B')$
   But using strong subadditivity $S(B') - S(A',B') \leq S(B',C') - S(A',B',C')$

   $$\implies S(A':B') \leq S(A') + S(B',C') - S(A',B',C') = S(A':B',C') = S(A:B,C) = S(A:B)$$

■