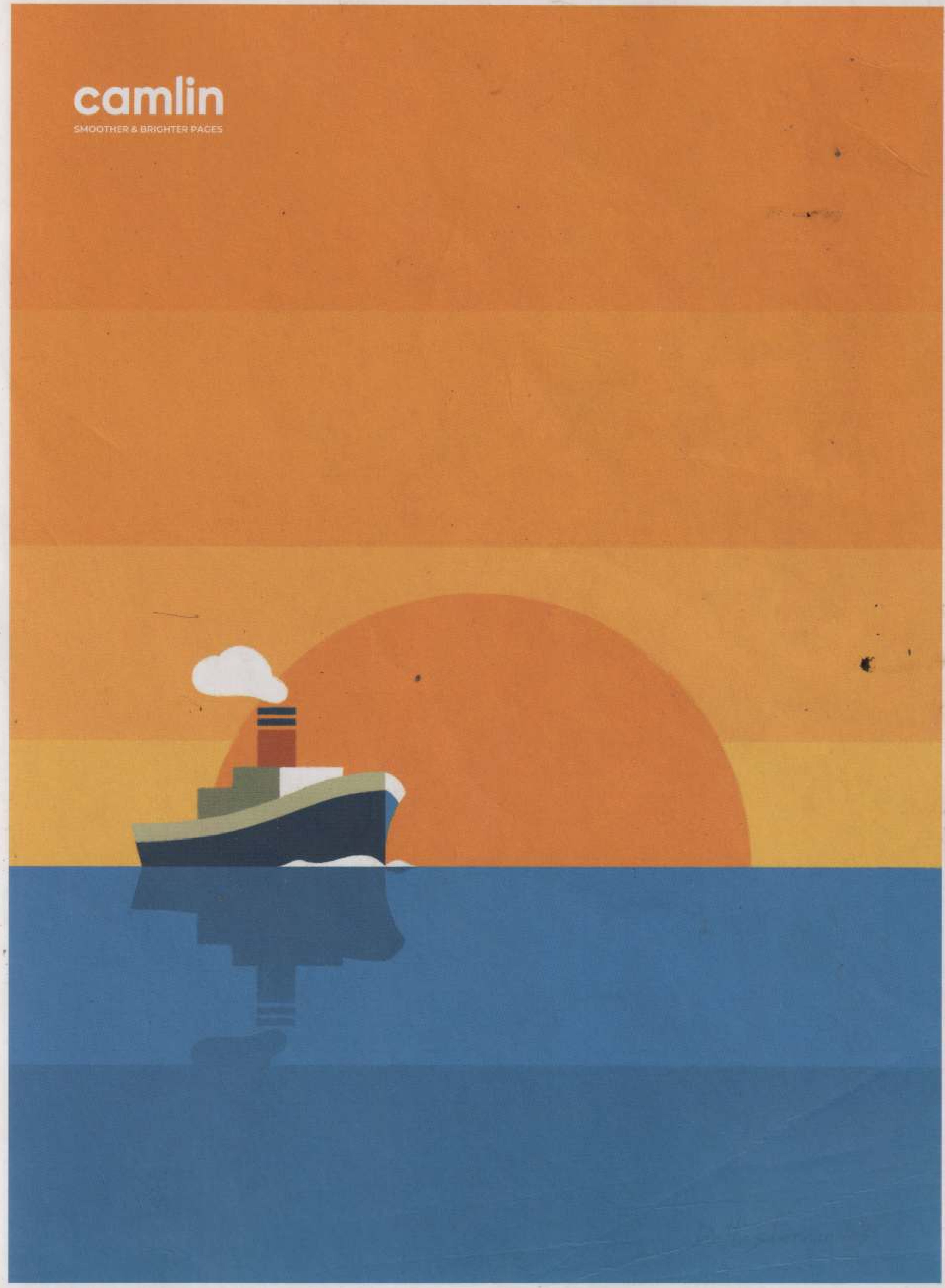
camlin
SMOOTHER & BRIGHTER PAGES

soorajss1729@gmail.com

+91-9400635788

INDEX

NAME SOORAJ·S· SUBJECT ______ 11·3

STD. ______ DIV. ______ ROLL NO. ______ SCHOOL ______

SR. NO.	PAGE NO.	TITLE	DATE	TEACHER'S SIGN / REMARKS
		QUANTUM COMPUTATION		
		& QUANTUM INFORMATION		
		– Nielsen & Chuang		

Ex: A 6.8 Let A be a +ve matrix. Define a superoperator (linear operator on matrices) by the equation $\mathcal{A}(X) \equiv AX$. Show that $\mathcal{A}$ is +ve w.r.t the Hilbert-Schmidt inner product. ie, for all X, $tr(X^{\dagger}\mathcal{A}(X)) \geq 0$.

Similarly, show that the superoperator defined by $\mathcal{A}(X) \equiv XA$ is +ve w.r.t the Hilbert Schmidt inner product on matrices.

Ans: A is a positive matrix $\Rightarrow x^{\dagger}Ax \geq 0 \quad \forall x$

Define, $\mathcal{A}(X) \equiv AX$

$XX^{\dagger}$ is positive matrix, since

$x^{\dagger}XX^{\dagger}x = (X^{\dagger}x)^{\dagger}(X^{\dagger}x) \geq 0$

If S & T are positive, so is ST

Since, $STx = \lambda x \Rightarrow (Tx)^{\dagger}STx = (Tx)^{\dagger}\lambda x = x^{\dagger}T^{\dagger}\lambda x = \lambda x^{\dagger}Tx$

$$\lambda = \frac{(Tx)^{\dagger}S(Tx) \geq 0}{x^{\dagger}Tx \geq 0} \geq 0$$

$\therefore XX^{\dagger}A$ is a positive matrix with non negative eigenvalues.

$tr(X^{\dagger}\mathcal{A}(X)) = tr(X^{\dagger}AX) = tr(XX^{\dagger}A) \geq 0.$

Theorem A6.1 :

Lieb's theorem : Let X be a matrix, and $0 \le t \le 1$.

Then the function

$$f(A,B) \equiv tr\left(X^{\dagger} A^{t} X B^{1-t}\right)$$

is jointly concave in positive matrices A and B.

$$tr\left[X^{\dagger}(\lambda A_1 + (1-\lambda) A_2)^{t} X (\lambda B_1 + (1-\lambda) B_2)^{1-t}\right]$$

$$\ge \lambda\, tr\left(X^{\dagger} A_1^{t} X B_1^{1-t}\right) + (1-t)\, tr\left(X^{\dagger} A_2^{t} X B_2^{1-t}\right)$$

Lemma A6.2

Let $R_1, R_2, S_1, S_2, T_1, T_2$ be positive operators such that $[R_1, R_2] = [S_1, S_2] = [T_1, T_2] = 0$, and

$$R_1 \geq S_1 + T_1$$

$$R_2 \geq S_2 + T_2$$

Then for all $0 \leq t \leq 1$,

$$R_1^t R_2^{1-t} \geq S_1^t S_2^{1-t} + T_1^t T_2^{1-t} \quad - \boxed{A6.8}$$

is true as a matrix inequality.

Proof

Assume that R_1 and R_2 are invertible

Let $|x\rangle$ and $|y\rangle$ be any 2 vectors.
Applying the Cauchy - Schwarz inequality,

$$|\langle u|v\rangle|^2 \leq \langle u|u\rangle\langle v|v\rangle \implies |\langle u|v\rangle| \leq \|u\| \cdot \|v\|$$

$$\left|\langle x|\left(S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2}\right)|y\rangle\right| = \left|\langle x|S_1^{1/2} S_2^{1/2}|y\rangle + \langle x|T_1^{1/2} T_2^{1/2}|y\rangle\right|$$

$$\leq \left|\langle x|S_1^{1/2} S_2^{1/2}|y\rangle\right| + \left|\langle x|T_1^{1/2} T_2^{1/2}|y\rangle\right|$$

$$\leq \|S_1^{1/2}|x\rangle\| \, \|S_2^{1/2}|y\rangle\| + \|T_1^{1/2}|x\rangle\| \, \|T_2^{1/2}|y\rangle\|$$

$$\|S_1^{1/2}|x\rangle\|^2 \|T_2^{1/2}|y\rangle\|^2 + \|S_2^{1/2}|y\rangle\|^2 \|T_1^{1/2}|x\rangle\|^2 - 2\|S_1^{1/2}|x\rangle\| \, \|S_2^{1/2}|y\rangle\| \, \|T_1^{1/2}|x\rangle\| \, \|T_2^{1/2}|y\rangle\|$$

$$= \left(\|S_1^{1/2}|x\rangle\| \, \|T_2^{1/2}|y\rangle\| - \|S_2^{1/2}|y\rangle\| \, \|T_1^{1/2}|x\rangle\|\right)^2 \geq 0.$$

$$\Rightarrow 2\|S_1^{1/2}|x\rangle\| \, \|S_2^{1/2}|y\rangle\| \, \|T_1^{1/2}|x\rangle\| \, \|T_2^{1/2}|y\rangle\| \leq \|S_1^{1/2}|x\rangle\|^2 \|T_2^{1/2}|y\rangle\|^2 + \|S_2^{1/2}|y\rangle\|^2 \|T_1^{1/2}|x\rangle\|^2$$

$$\leq \sqrt{\left(\|S_1^{1/2}|x\rangle\|^2 + \|T_1^{1/2}|x\rangle\|^2\right)\left(\|S_2^{1/2}|y\rangle\|^2 + \|T_2^{1/2}|y\rangle\|^2\right)}$$

$$= \sqrt{\langle x|S_1 + T_1|x\rangle\langle y|S_2 + T_2|y\rangle}$$

$$\leq \sqrt{\langle x|R_1|x\rangle\langle y|R_2|y\rangle}$$

since, $S_1 + T_1 \leq R_1$ and $S_2 + T_2 \leq R_2$

$\therefore$

$$\left|\langle x|\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)|y\rangle\right| \leq \sqrt{\langle x|R_1|x\rangle\langle y|R_2|y\rangle}$$

Let $|u\rangle$ be any unit vector, and defining $|x\rangle \equiv R_1^{-1/2}|u\rangle$ and $|y\rangle \equiv R_2^{-1/2}|u\rangle$ gives,

$$\left|\langle u|R_1^{-1/2}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/2}|u\rangle\right|$$

$$\leq \sqrt{\langle u|R_1^{-1/2}R_1R_1^{-1/2}|u\rangle\langle u|R_2^{-1/2}R_2R_2^{-1/2}|u\rangle}$$

$$= \sqrt{\langle u|u\rangle\langle u|u\rangle} = 1$$

for all unit vectors $|u\rangle$.

$$\|A\| = \max_{\langle u|u\rangle=1} |\langle u|A|u\rangle|$$

$\therefore$

$$\left\|R_1^{-1/2}\left(S_1^{1/2}S_2^{1/2}+T_1^{1/2}T_2^{1/2}\right)R_2^{-1/2}\right\| \leq 1$$

Define, $A \equiv R_1^{-1/4} R_2^{-1/4} \left(S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2}\right) R_2^{-1/2}$

$B \equiv R_2^{1/4} R_1^{-1/4}$

[A6.6] AB is hermitian $\Rightarrow \|AB\| = \|BA\|$

$$\|AB\| = \left\| R_1^{-1/4} R_2^{-1/4} \left(S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2}\right) R_2^{-1/2} R_1^{-1/4} \right\|$$

$$= \|BA\|$$

$$= \left\| R_1^{-1/2} \left(S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2}\right) R_2^{-1/2} \right\|$$

$$\leq 1$$

[A6.7] Given A is positive. $\|A\| \leq 1$ iff $A \leq I$.

$\therefore$

$$R_1^{-1/4} R_2^{-1/4} \left(S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2}\right) R_2^{-1/2} R_1^{-1/4} \leq I$$

$$R_1^{-1/2} \left(S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2}\right) R_2^{-1/2} \leq I$$

$\boxed{A6.1}$ $A \le B \longrightarrow XAX^\dagger \le XBX^\dagger \quad \forall\, X$

Take $X = R_2^{1/4} R_1^{1/4}$,

$$S_1^{1/2} S_2^{1/2} + T_1^{1/2} T_2^{1/2} \le R_1^{1/2} R_2^{1/2} \qquad \boxed{[R_1, R_2] = 0}$$

$\therefore$

$R_1^{t} R_2^{1-t} \ge S_1^{t} S_2^{1-t} + T_1^{t} T_2^{1-t}$ holds for $t = 1/2$.

Let I be the set of all t such that (A6.8) holds.

$R_1 \ge S_1 + T_1$ & $R_2 \ge S_2 + T_2$

$\Longrightarrow$ 0 and 1 are elements of I

and $1/2$ is also an element of I.

Suppose μ and η are any 2 elements of I, so that

$$R_1^{\mu} R_2^{1-\mu} \geq S_1^{\mu} S_2^{1-\mu} + T_1^{\mu} T_2^{1-\mu}$$

$$R_1^{\eta} R_2^{1-\eta} \geq S_1^{\eta} S_2^{1-\eta} + T_1^{\eta} T_2^{1-\eta}$$

$R_1^{\mu} R_2^{1-\mu}$, $S_1^{\mu} S_2^{1-\mu}$, $T_1^{\mu} T_2^{1-\mu}$, $R_1^{\eta} R_2^{1-\eta}$, $S_1^{\eta} S_2^{1-\eta}$, $T_1^{\eta} T_2^{1-\eta}$ are positive operators.

$$\left[R_1^{\mu} R_2^{1-\mu}, R_1^{\eta} R_2^{1-\eta}\right] = R_1^{\mu} R_2^{1-\mu} R_1^{\eta} R_2^{1-\eta} - R_1^{\eta} R_2^{1-\eta} R_1^{\mu} R_2^{1-\mu}$$
$$= 0$$

$$\left[S_1^{\mu} S_2^{1-\mu}, S_1^{\eta} S_2^{1-\eta}\right] = 0 = \left[T_1^{\mu} T_2^{1-\mu}, T_1^{\eta} T_2^{1-\eta}\right]$$

$\therefore$

Using the already proven $t = 1/2$ case,

$$\left(R_1^{\mu} R_2^{1-\mu}\right)^{1/2} \left(R_1^{\eta} R_2^{1-\eta}\right)^{1/2} \geq \left(S_1^{\mu} S_2^{1-\mu}\right)^{1/2} \left(S_1^{\eta} S_2^{1-\eta}\right)^{1/2} + \left(T_1^{\mu} T_2^{1-\mu}\right)^{1/2} \left(T_1^{\eta} T_2^{1-\eta}\right)^{1/2}$$

Using the commutativity assumptions

$$[R_1, R_2] = [S_1, S_2] = [T_1, T_2] = 0 \quad \text{and} \quad \nu \equiv \frac{\mu+\eta}{2},$$

$$R_1^{\nu} R_2^{1-\nu} \geq S_1^{\nu} S_2^{1-\nu} + T_1^{\nu} T_2^{1-\nu}$$

$\Rightarrow$ Whenever μ and η are in I, so is $\frac{\mu+\eta}{2}$.

and $\{0, 1/2, 1\} \in I$.

28/8/2023

A number $t_n \in [0,1]$ with a finite binary expansion (dyadic rationals) can be written as,

$$t_n = 0.\phi_1\phi_2\phi_3 \cdots = \frac{\phi_1}{2^1} + \frac{\phi_2}{2^2} + \frac{\phi_3}{2^3} + \cdots + \frac{\phi_n}{2^n}$$

$$= \frac{1}{2}\left[\phi_1 + \frac{\phi_2}{2^1} + \frac{\phi_3}{2^2} + \frac{\phi_4}{2^3} + \cdots + \frac{\phi_n}{2^{n-1}}\right]$$

$$= \frac{1}{2}\left[\phi_1 + \frac{1}{2}\left[\phi_2 + \frac{\phi_3}{2} + \frac{\phi_4}{2^2} + \frac{\phi_5}{2^3} + \cdots + \frac{\phi_n}{2^{n-2}}\right]\right]$$

$$= \frac{1}{2}\left[\phi_1 + \frac{1}{2}\left[\phi_2 + \frac{1}{2}\left[\phi_3 + \frac{\phi_4}{2^1} + \frac{\phi_5}{2^2} + \frac{\phi_6}{2^3} + \cdots + \frac{\phi_n}{2^{n-3}}\right]\right]\right]$$

$$= \frac{1}{2}\left[\phi_1 + \frac{1}{2}\left[\phi_2 + \frac{1}{2}\left[\phi_3 + \cdots + \frac{1}{2}\left[\phi_{n-3} + \frac{1}{2}\left(\phi_{n-2} + \frac{1}{2}\left(\phi_{n-1} + \frac{\phi_n}{2}\right)\right)\right]\right]\right]\right]$$

where $\phi_1, \phi_2, \ldots, \phi_n \in \{0, 1\}$.

Looking at the inner most term $\frac{1}{2}\left(\phi_{n-1} + \frac{\phi_n}{2}\right)$ in which $\phi_{n-1} \in \{0,1\}$ and $\frac{\phi_n}{2} \in \{0, 1/2\}$, ie., $\phi_{n-1}, \frac{\phi_n}{2} \in I$, and therefore $\frac{1}{2}\left(\phi_{n-1} + \frac{\phi_n}{2}\right) \in I$.

In the next term, $\frac{1}{2}\left[\phi_{n-2} + \frac{1}{2}\left(\phi_{n-1} + \frac{\phi_n}{2}\right)\right]$ has $\frac{1}{2}\left(\phi_{n-1} + \frac{\phi_n}{2}\right) \in I$ (as shown in the last step) and $\phi_{n-2} \in I$, and therefore $\frac{1}{2}\left[\phi_{n-2} + \frac{1}{2}\left(\phi_{n-1} + \frac{\phi_n}{2}\right)\right] \in I$.

Continuing this way we can prove that any # $t_n = 0.\phi_1\phi_2\cdots\phi_n = \frac{\phi_1}{2} + \frac{\phi_2}{2^2} + \cdots + \frac{\phi_n}{2^n} = \frac{k}{2^n}$ with finite binary expansion (dyadic rationals) is a member of I.

* Let $A \subseteq \mathbb{R}$ be a set that is bounded above. Then a number $\alpha \in \mathbb{R}$ is called the supremum (least upper bound) of A, denoted as $\sup A$ iff

- $x \leq \alpha \quad \forall\, x \in A$
- if y is an upper bound for A, then $y \geq \alpha$

* Let $A \subseteq \mathbb{R}$ be a set that is bounded below. Then a number $\beta \in \mathbb{R}$ is called the infimum (greatest lower bound) of A, denoted as $\inf A$ iff

- $x \geq \beta \quad \forall\, x \in A$
- if y is a lower bound for A, then $y \leq \beta$

* The Completeness axiom:

Every non-empty subset A of $\mathbb{R}$ that is bounded above has a least upper bound. That is, $\sup A$ exists and is a real number.

* The Archimedean property:

For any $x \in \mathbb{R}$, there exists $n \in \mathbb{N}$ such that $n > x$.

Equivalently,

for any $x \in \mathbb{R}$ with $x > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < x$.

Proof

Let $x \in \mathbb{R}$. Suppose the converse is true, ie., there doesn't exist $n \in \mathbb{N}$ such that $n > x$.

That is,

$$n \leq x \quad \forall \quad n \in \mathbb{N}$$

$\Rightarrow$ $\mathbb{N} \in \mathbb{R}$ is bounded above by x

$\Rightarrow \mathbb{N}$ has a least upper bound, $\alpha = \sup(\mathbb{N}) \in \mathbb{R}$

(by the completeness axiom).

$\Rightarrow \alpha - 1 < \alpha$ and therefore

$\alpha - 1$ is not an upper bound for $\mathbb{N}$.

$\Rightarrow$ There exists $m \in \mathbb{N}$ such that

$\alpha - 1 < m \leq \alpha$

$\Rightarrow \alpha < m + 1 \in \mathbb{N}$

which contradicts ~~the~~ fact that α is an upper bound of $\mathbb{N}$.

* Lemma 1: For $\delta > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{2^n} < \delta$.

Proof

Substitute $x = \delta$ in the Archimedean property, obtains $\frac{1}{2^n} < \frac{1}{n} < \delta$.

* $X \subset Y$ is dense in Y if for any $\delta > 0$ and $y \in Y$, there is some $x \in X$ such that $|y - x| < \delta$

We have to prove that the set $\left\{ \frac{k}{2^n} \,\middle|\, k \in \mathbb{W}, n \in \mathbb{N}, 0 \leq k \leq 2^n \right\}$ of dyadic rationals, ie., numbers with binary expansion in $[0,1]$, are dense in $[0,1]$.

Let's take any $\delta > 0$, then from lemma 1 there exists $n \in \mathbb{N}$ such that $\frac{1}{2^n} < \delta$.

Let $x \in [0,1]$ and $k = \lfloor x \cdot 2^n \rfloor$ corresponds to the greatest integer less than or equal to $x \cdot 2^n$ such that $0 < k \leq 2^n$.

$$k = \lfloor x \cdot 2^n \rfloor \leq x \cdot 2^n \leq k+1 = \lfloor x \cdot 2^n \rfloor + 1$$

$$\implies \frac{k}{2^n} \leq x \leq \frac{k+1}{2^n}$$

$$\implies 0 \leq x - \frac{k}{2^n} \leq \frac{1}{2^n} < \delta \quad \text{(Lemma 1)}$$

$\therefore$ For any $\delta > 0$ and $x \in [0,1]$ there is some $\frac{k}{2^n} \in \left\{ \frac{k}{2^n} \middle| k \in W, n \in \mathbb{N}, 0 \leq k \leq 2^n \right\}$ such that $\left| x - \frac{k}{2^n} \right| < \delta$.

$\implies$ The set $\left\{ \frac{k}{2^n} \middle| k \in W, n \in \mathbb{N}, 0 \leq k \leq 2^n \right\}$ is dense in $[0,1]$

$\implies I$ is dense in $[0,1]$

$\therefore$

Part 1 proves that dyadic rationals are members of I, and in part 2 we have proven that the dyadic rationals are dense in $[0,1]$.

ie.,

We can approach any $t \in [0,1]$ by a sequence in our already established I which contains the dyadic rationals. Therefore, the validity of the equations for $t \in [0,1]$ is proven.

Lieb's theorem

Let X be a matrix, and $0 \leq t \leq 1$. Then the function

$$f(A, B) \equiv tr\left(X^{\dagger} A^{t} X B^{1-t}\right)$$

is jointly concave in positive matrices A and B.

ie;

$$f\left(\lambda A_1 + (1-\lambda) A_2, \lambda B_1 + (1-\lambda) B_2\right) \geq \lambda f(A_1, B_1) + (1-\lambda) f(A_2, B_2) \quad \forall \lambda \in [0,1]$$

$$tr\left[X^{\dagger}\left(\lambda A_1 + (1-\lambda) A_2\right)^{t} X \left(\lambda B_1 + (1-\lambda) B_2\right)^{1-t}\right] \geq$$

$$\lambda\, tr\left(X^{\dagger} A_1^{t} X B_1^{1-t}\right) + (1-\lambda)\, tr\left(X^{\dagger} A_2^{t} X B_2^{1-t}\right)$$

Proof

Let $0 \leq \lambda \leq 1$ and define superoperators (linear maps on operators) $S_1, S_2, T_1, T_2, R_1, R_2$ as follows:

$$S_1(X) \equiv \lambda A_1 X$$

$$S_2(X) \equiv \lambda X B_1$$

$$T_1(X) \equiv (1-\lambda) A_2 X$$

$$T_2(X) \equiv (1-\lambda) X B_2$$

$$R_1 \equiv S_1 + T_1$$

$$R_2 \equiv S_2 + T_2$$

$$S_1 S_2(X) = S_1(\lambda X B_1) = \lambda A_1 \cdot \lambda X B_1 = \lambda^2 A_1 X B_1$$

$$S_2 S_1(X) = S_2(\lambda A_1 X) = \lambda \cdot \lambda A_1 X \cdot B_1 = \lambda^2 A_1 X B_1$$

S_1 and S_2 commute, as do T_1 and T_2, and R_1 and R_2.

Ex (A.6.8)

- Let A be a +ve matrix. The superoperator (linear operator on matrices) defined by the equation $\mathcal{A}(X) \equiv AX$, is +ve w.r.t the Hilbert-Schmidt inner product, ie., $tr(X^\dagger \mathcal{A}(X)) \geq 0 \quad \forall X$. The superoperator defined by $\mathcal{A}(X) \equiv XA$ is +ve w.r.t the Hilbert-Schmidt inner product on matrices.

A_1, B_1, A_2, B_2 are +ve matrices

$\Rightarrow S_1, S_2, T_1, T_2, R_1, R_2$ are +ve w.r.t the Hilbert-Schmidt inner product.

$\therefore$

Lemma $\Rightarrow \quad R_1^t R_2^{1-t} \geq S_1^t S_2^{1-t} + T_1^t T_2^{1-t}$

$$(S_1+T_1)^t (S_2+T_2)^{1-t} \geq S_1^t S_2^{1-t} + T_1^t T_2^{1-t}$$

$$\Rightarrow R_1^t R_2^{1-t} - S_1^t S_2^{1-t} - T_1^t T_2^{1-t} \geq 0$$

$\Rightarrow R_1^t R_2^{1-t} - S_1^t S_2^{1-t} - T_1^t T_2^{1-t}$ is positive

Ex A6.8 $\Rightarrow$ Given A is +ve and $\mathcal{A}(X) \equiv AX$ then $\mathcal{A}$ is +ve w.r.t the Hilbert-Schmidt inner product, ie, $tr(X^\dagger \mathcal{A}(X)) = 0 \quad \forall X$.

$\therefore$

$$tr\left[X^\dagger \left(R_1^t R_2^{1-t} - S_1^t S_2^{1-t} - T_1^t T_2^{1-t}\right)(X)\right] \geq 0$$

$$tr\left[X^\dagger \left(R_1^t(X) R_2^{1-t}(X) - S_1^t(X) S_2^t(X) - T_1^t(X) T_2^{1-t}(X)\right)\right] \geq 0$$

$$tr\left[X^\dagger \left(\lambda A_1 X + (1-\lambda)A_2 X\right)^t \left(\lambda X B_1 + (1-\lambda) X B_2\right)^{1-t} - (\lambda A_1 X)^t (\lambda X B_1)^{1-t} - \left((1-\lambda)A_2 X\right)^t \left((1-\lambda) X B_2\right)^{1-t}\right] \geq 0$$

$$\operatorname{tr}\left[X^{\dagger}(\lambda A_1+(1-\lambda)A_2)^{t} X (\lambda B_1+(1-\lambda)B_2)^{1-t}\right]$$
$$- \operatorname{tr}\left[X^{\dagger}(\lambda A_1)^{t} X (\lambda B_1)^{1-t}\right]$$
$$- \operatorname{tr}\left[X^{\dagger}((1-\lambda)A_2)^{t} X ((1-\lambda)B_2)^{1-t}\right] \geq 0$$

$$\operatorname{tr}\left[X^{\dagger}(\lambda A_1+(1-\lambda)A_2)^{t} X (\lambda B_1+(1-\lambda)B_2)^{1-t}\right]$$
$$-\lambda \operatorname{tr}\left[X^{\dagger} A_1^{t} X B_1^{1-t}\right] - (1-\lambda)\operatorname{tr}\left[X^{\dagger} A_2^{t} X B_2^{1-t}\right] \geq 0$$

$\therefore$

$$\operatorname{tr}\left(X^{\dagger}(\lambda A_1+(1-\lambda))^{t} X (\lambda B_1+(1-\lambda)B_2)^{1-t}\right]$$
$$\geq \lambda \operatorname{tr}\left(X^{\dagger} A_1^{t} X B_1^{1-t}\right) - (1-\lambda)\operatorname{tr}\left(X^{\dagger} A_2^{t} X B_2^{1-t}\right)$$

* The relative entropy $S(\rho \| \sigma)$ is jointly convex in its arguments.

where,

$$S(\rho\|\sigma) = tr(\rho \log \rho) - tr(\rho \log \sigma)$$
$$= -S(\rho) - tr(\rho \log \sigma)$$
$$= tr\, \rho(\log \rho - \log \sigma)$$

Proof

For arbitrary matrices A and X acting on the same space, define

$$I_t(A,X) \equiv tr(X^\dagger A^t X A^{1-t}) - tr(X^\dagger X A)$$

Lieb's theorem $\Rightarrow$ $tr(X^\dagger A^t X A^{1-t})$ is concave in A

$$tr\left(X^\dagger(\lambda A_1 + (1-\lambda)A_2)^t X (\lambda A_1 + (1-\lambda)A_2)^{1-t}\right)$$
$$\geq \lambda\, tr(X^\dagger A_1^t X A_1^{1-t}) + (1-\lambda)\, tr(X^\dagger A_2^t X A_2^{1-t})$$

$$tr\left(X^{\dagger}X\left(\lambda A_1+(1-\lambda)A_2\right)\right) = tr\left(\lambda X^{\dagger}X A_1 + (1-\lambda)X^{\dagger}X A_2\right)$$

$$= tr\left(\lambda X^{\dagger}X A_1\right) + tr\left((1-\lambda)X^{\dagger}X A_2\right)$$

$$= \lambda\, tr\left(X^{\dagger}X A_1\right) + (1-\lambda)\, tr\left(X^{\dagger}X A_2\right)$$

$\Longrightarrow tr\left(X^{\dagger}XA\right)$ is linear in A.

$$\therefore\quad I_t\left(\lambda A_1+(1-\lambda)A_2, X\right) \geq \lambda I_2(A_1, X) + (1-\lambda) I_2(A_2, X)$$

$\Longrightarrow I_t(A, X)$ is concave in A.

Q-Stack
4/4/2023

$F(t)$: each element of the matrix depends on the parameter t.

$$\frac{d}{dt}\operatorname{tr}\left(F(t)\right) = \frac{d}{dt}\sum_i F_{ii}(t) = \sum_i \frac{d}{dt}F_{ii}(t) = \operatorname{tr}\left(\frac{d}{dt}F(t)\right)$$

A is hermitian $\Longrightarrow$ $A = VDV^{\dagger} = V\begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix}V^{\dagger}$

$$A^t = VD^tV^{\dagger} = V\begin{bmatrix} d_1^t & & \\ & \ddots & \\ & & d_n^t \end{bmatrix}V^{\dagger}$$

$$\frac{d}{dt}A^t = V\frac{d}{dt}D^tV^{\dagger} = V\begin{bmatrix} \frac{d}{dt}d_1^t & & \\ & \ddots & \\ & & \frac{d}{dt}d_n^t \end{bmatrix}V^{\dagger} = V\begin{bmatrix} d_1^t\log d_1 & & \\ & \ddots & \\ & & d_n^t\log d_n \end{bmatrix}V^{\dagger}$$

$$= V\begin{bmatrix} \log d_1 & & \\ & \ddots & \\ & & \log d_n \end{bmatrix}\begin{bmatrix} d_1^t & & \\ & \ddots & \\ & & d_n^t \end{bmatrix}V^{\dagger} = V(\log D)D^tV^{\dagger}$$

$$= V\log D\,V^{\dagger}V\,D^t\,V^{\dagger} = \log(A)\,A^t$$

$$\frac{d}{dt} A^t = \frac{d}{dt} e^{\log A^t} = \frac{d}{dt} e^{t \log A} = \log(A) \times e^{t \log A}$$

$$= \log(A)\, A^t$$

$$\therefore \quad I_t(A,X) = tr\left(X^\dagger A^t X A^{1-t}\right) - tr\left(X^\dagger X A\right)$$

$$\frac{d}{dt} I_t(A,X) = \frac{d}{dt}\, tr\left(X^\dagger A^t X A^{1-t}\right)$$

$$= tr\left(\frac{d}{dt}\left(X^\dagger A^t X A^{1-t}\right)\right)$$

$$= tr\left[X^\dagger\left(\frac{d}{dt} A^t\right) X A^{1-t} + X^\dagger A^t X \left(\frac{d}{dt} A^{1-t}\right)\right]$$

$$= tr\left[X^\dagger \log(A)\, A^t X A^{1-t}\right] - tr\left[X^\dagger A^t X \log(A)\, A^{1-t}\right]$$

Define,

$$\underline{I}(A,X) = \left.\frac{d}{dt}\right|_{t=0} I_t(A,X)$$

$$= tr\left(X^\dagger (\log A) X A\right) - tr\left(X^\dagger X (\log A) A\right)$$

$I_0(A, X) = 0$ and $I_t(A, X)$ is concave in A,

$$\frac{d}{dt} I_t(A, X) = \lim_{\delta t \to 0} \frac{I_{t+\delta t}(A, X) - I_t(A, X)}{\delta t}$$

$$\left.\frac{d}{dt}\right|_{t=0} I_t(A, X) = \lim_{\delta t \to 0} \frac{I_{\delta t}(A, X) - I_0(A, X)}{\delta t}$$

$\therefore$

$$I(\lambda A_1 + (1-\lambda) A_2, X) = \left.\frac{d}{dt}\right|_{t=0} I_t(\lambda A_1 + (1-\lambda) A_2, X)$$

$$= \lim_{\Delta \to 0} \frac{I_\Delta(\lambda A_1 + (1-\lambda) A_2, X)}{\Delta}$$

$$\geq \lambda \lim_{\Delta \to 0} \frac{I_\Delta(A_1, X)}{\Delta} + (1-\lambda) \lim_{\Delta \to 0} \frac{I_\Delta(A_2, X)}{\Delta}$$

$$= \lambda \left.\frac{d}{dt}\right|_{t=0} I_t(A_1, X) + (1-\lambda) \left.\frac{d}{dt}\right|_{t=0} I_t(A_2, X)$$

$$= \lambda I(A_1, X) + (1-\lambda) I(A_2, X)$$

$\Rightarrow I(A, X)$ is a concave function of A.

Defining the block matrices,

$$A = \begin{bmatrix} \rho & 0 \\ 0 & \sigma \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix}$$

$$A = \begin{bmatrix} \rho & 0 \\ 0 & \sigma \end{bmatrix} = \begin{bmatrix} VDV^\dagger & 0 \\ 0 & U\Lambda U^\dagger \end{bmatrix} = \begin{bmatrix} V & 0 \\ 0 & U \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & \Lambda \end{bmatrix} \begin{bmatrix} V & 0 \\ 0 & U \end{bmatrix}^\dagger$$

$$= W \begin{bmatrix} D & 0 \\ 0 & \Lambda \end{bmatrix} W^\dagger$$

$$\log A = W \log \begin{bmatrix} D & 0 \\ 0 & \Lambda \end{bmatrix} W^\dagger = W \begin{bmatrix} \log D & 0 \\ 0 & \log \Lambda \end{bmatrix} W^\dagger$$

$$= \begin{bmatrix} V \log D\, V^\dagger & 0 \\ 0 & U \log \Lambda\, U^\dagger \end{bmatrix} = \begin{bmatrix} \log \rho & 0 \\ 0 & \log \sigma \end{bmatrix}$$

$\therefore$

$$X^\dagger (\log A) X A = \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \log \rho & 0 \\ 0 & \log \sigma \end{bmatrix} \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix} \begin{bmatrix} \rho & 0 \\ 0 & \sigma \end{bmatrix}$$

$$= \begin{bmatrix} 0 & \log \sigma \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \rho & 0 \end{bmatrix} = \begin{bmatrix} (\log \sigma)\rho & 0 \\ 0 & 0 \end{bmatrix}$$

$$\Rightarrow \operatorname{tr}\left(X^\dagger (\log A) X A\right) = \operatorname{tr}\left[(\log \sigma)\rho\right] = \operatorname{tr}\left[\rho \log \sigma\right]$$

$$X^\dagger X(\log A)A = \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix}\begin{bmatrix} \log\rho & 0 \\ 0 & \log\sigma \end{bmatrix}\begin{bmatrix} \rho & 0 \\ 0 & \sigma \end{bmatrix}$$

$$= \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} (\log\rho)\rho & 0 \\ 0 & (\log\sigma)\sigma \end{bmatrix} = \begin{bmatrix} (\log\rho)\rho & 0 \\ 0 & 0 \end{bmatrix}$$

$$\Rightarrow \mathrm{tr}\left(X^\dagger X(\log A)A\right) = \mathrm{tr}\left[(\log\rho)\rho\right] = \mathrm{tr}\left[\rho\log\rho\right]$$

$\therefore$

$$I(A,X) = \mathrm{tr}\left(X^\dagger(\log A)XA\right) - \mathrm{tr}\left(X^\dagger X(\log A)A\right)$$

$$= \mathrm{tr}(\rho\log\sigma) - \mathrm{tr}(\rho\log\rho)$$

$$= -S(\rho\|\sigma)$$

$I(A,X)$ is concave $\Rightarrow -S(\rho\|\sigma)$ is concave

$\Rightarrow S(\rho\|\sigma)$ is jointly convex.

*

Let AB is a composite quantum system with components A and B. Then,

the conditional entropy $S(A|B)$ is concave in the state ρ^{AB} of AB.

ie., If ρ_1^{AB} and ρ_2^{AB} are quantum bipartite states of the system AB, and $\lambda \in [0,1]$ then

$$S(A|B)_{\lambda\rho_1^{AB}+(1-\lambda)\rho_2^{AB}} \geq \lambda S(A|B)_{\rho_1^{AB}} + (1-\lambda) S(A|B)_{\rho_2^{AB}}$$

Proof

Let d be the dimension of system A.

$$S(\rho\|\sigma) = -S(\rho) - tr(\rho \log \sigma)$$

$$S(\rho^{AB}\|I/d\otimes\rho^B) = -S(A,B) - tr(\rho^{AB}\log(I/d\otimes\rho^B))$$

$$\log(\rho^A\otimes\rho^B) = \log(\rho^A)\otimes I_B + I_A\otimes\log(\rho^B)$$

$$= -S(A,B) - tr\left[\rho^{AB}\left(\log I/d\otimes I_B + I_A\otimes\log\rho^B\right)\right]$$

$$= -S(A,B) - tr\left(\rho^{AB}\left(\log I/d\otimes I_B\right)\right) - tr\left(\rho^{AB}\left(I_A\otimes\log\rho^B\right)\right)$$

QC (11.2)
QC (2)

$$tr\left(\rho^{AB}(M\otimes I_B)\right) = tr\left(M\rho^{A}\right)$$

$$tr\left(\rho^{AB}(I_A\otimes M)\right) = tr\left(M\rho^{B}\right)$$

$$\therefore \quad tr\left(\rho^{AB}(\log I/d \otimes I_B)\right) = tr\left(\rho^{A}\log I/d\right)$$

$$= tr\left(\rho^{A}(\log 1/d)\, I\right)$$

$$= (\log 1/d)\, tr\left(\rho^{A}\right) = -\log d$$

$$tr\left(\rho^{AB}(I_A\otimes \log\rho^{B})\right) = tr\left(\rho^{B}\log\rho^{B}\right)$$

$$\therefore \quad S\left(\rho^{AB}\,\|\, I/d\otimes\rho^{B}\right) = -S(A,B) - tr\left(\rho^{B}\log\rho^{B}\right) + \log d$$

$$= -S(A,B) + S(B) + \log d$$

$$= -S(A|B) + \log d$$

$$\therefore \quad S(A|B) = \log d - S\left(\rho^{AB}\,\|\, I/d\otimes\rho^{B}\right)$$

$S\left(\rho^{AB}\,\|\, I/d\otimes\rho^{B}\right)$ is jointly convex

$\Longrightarrow S(A|B)$ is jointly concave.

* Theorem 11.14: Strong subadditivity

For any trio of quantum systems A, B, C, the following inequalities hold.

$$\boxed{\begin{aligned} S(A)+S(B) &\le S(A,C)+S(B,C) \\ S(A,B,C)+S(B) &\le S(A,B)+S(B,C) \end{aligned}}$$

Proof.

Define a function $T(\rho^{ABC})$ of density operators on the system ABC,

$$T(\rho^{ABC}) = S(A)+S(B)-S(A,C)-S(B,C) = -S(C|A)-S(C|B)$$

$$\left[\begin{aligned} S(C|A) &= S(A,C)-S(A) \\ S(C|B) &= S(B,C)-S(B) \end{aligned}\right.$$

Conditional entropy is concave $\Rightarrow$ $T(\rho^{ABC})$ is a convex function of ρ^{ABC}.

Let the spectral decomposition of ρ^{ABC} be,

$$\rho^{ABC} = \sum_i p_i |i\rangle\langle i| .$$

T is a convex of ρ^{ABC}

$$T(\rho^{ABC}) = T\left(\sum_i p_i |i\rangle\langle i|\right) \le \sum_i p_i \, T(|i\rangle\langle i|)$$

ρ is pure $\longleftrightarrow$ $S(\rho) = 0$

AB is a pure state $\longrightarrow$ $S(A) = S(B)$

$$S(A|C) = S(A,C) - S(C)$$

$\therefore$ $\rho_i^{ABC} = |i\rangle\langle i|$ is a pure state $\Longrightarrow$ $S(A,C) = S(B)$, $S(B,C) = S(A)$

$$T(\rho^{ABC}) \equiv S(A) + S(B) - S(A,C) - S(B,C)$$

$$\therefore \; T(\rho_i^{ABC}) = T(|i\rangle\langle i|) = 0$$

$\therefore$

$$T(\rho^{ABC}) = T\left(\sum_i p_i |i\rangle\langle i|\right) \leq 0$$

$\therefore$

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

$$\Rightarrow S(A) + S(B) \leq S(A,C) + S(B,C)$$

Introduce an auxiliary system R purifying the system ABC.

$$S(R) + S(B) \leq S(R,C) + S(B,C)$$

ABCR is a pure state $\Rightarrow$ $S(R) = S(ABC)$
$S(R,C) = S(A,B)$

$$\therefore S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$$

Ex: 11.24 Show that the inequality $S(A)+S(B) \le S(A,C)+S(B,C)$ can be obtained as a consequence of strong subadditivity, $S(A,B,C)+S(B) \le S(A,B)+S(B,C)$.

Ans: Given a system ABC, introduce another auxiliary system to purify ABC.
such that $|RABC\rangle$ is a pure state.

Strong subadditivity $\Rightarrow S(R,B,C)+S(B) \le S(R,B)+S(B,C)$

$|RABC\rangle$ is pure $\Rightarrow S(R,B,C) = S(A)$
$S(R,B) = S(A,C)$

$\therefore$

$S(A)+S(B) \le S(A,C)+S(B,C)$

Strong subadditivity : elementary applications

$S(A) + S(B) \leq S(A,C) + S(B,C)$ holds for both Shannon and von Neumann entropies., but for different reasons.

For Shannon entropy,

$$\left.\begin{aligned} H(A) &\leq H(A,C) \\ H(B) &\leq H(B,C) \end{aligned}\right\} H(A) + H(B) \leq H(A,C) + H(B,C)$$

For quantum von Neumann entropy,

Let $|AB\rangle$ is a pure state of a comp- system and $|AB\rangle$ is entangled.

$\therefore$

$B(\rho^{AB}) = 0$ where ρ^{AB} is pure.

ρ^{AB} is entangled $\longrightarrow$ ρ^{A}, ρ^{B} mixed state.

$\therefore \; S(\rho^{A}) > 0$ & $S(\rho^{B}) > 0$

$$S(B|A) = S(A,B) - S(A) = 0 - S(A) = -S(A) < 0.$$

$\therefore$

ρ^{AB} entangled $\Rightarrow$ $S(B|A) < 0$.

$\therefore \; S(A,B) - S(A) < 0$

$\Rightarrow \; \underline{S(A) > S(A,B)}$.

In the quantum case, it is possible to have either $S(A) > S(A,C)$ or $S(B) > S(B,C)$, yet somehow Nature conspires in such a way that both of these possibilities are not ~~true~~ simultaneously, in order to ensure that $S(A)+S(B) \leq S(A,C)+S(B,C)$ is always satisfied.

$$S(A)+S(B) \le S(A,C)+S(B,C)$$

$$\Rightarrow 0 \le S(A,C) - S(A) + S(B,C) - S(B)$$

$$\Rightarrow \boxed{0 \le S(C|A) + S(C|B)}$$

<u>Ex: 11.26</u> Prove that $S(A:B)+S(A:C) \le 2S(A)$.
The corresp. inequality for Shannon entropies holds since $H(A:B) \le H(A)$.
Find an example where $S(A:B) > S(A)$

Ans: $S(A:B) = S(A)+S(B)-S(A,B)$
$= S(A) - S(A|B)$ & $S(A:C) = S(A) - S(A|C)$

$S(A|B) = S(A,B) - S(B)$

$$S(A:B) + S(A:C) = S(A) - S(A|B) + S(A) - S(A|C)$$

$$= 2S(A) - \left(S(A|B) + S(A|C)\right)$$

$$\leq 2S(A).$$

since, $S(A|B) + S(A|C) \geq 0$

$$\therefore \boxed{S(A:B) + S(A:C) \leq 2S(A)}$$

$$S(A:B) > S(A) \implies S(A) - S(A|B) > S(A)$$

$$\implies -S(A|B) > 0 \implies S(A|B) < 0$$

Ex:- $|AB\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

$$\rho^{AB} = \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right)$$

$$= \frac{1}{2}\left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\right)$$

$$\rho^{A} = tr_B\left(\rho^{AB}\right) = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = I$$

$S(A,B) = 0$ since ρ^{AB} is a pure state.

$S(A) = S(B) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{2}\log\frac{1}{2} = 1$

$S(A:B) = S(A) + S(B) - S(A,B)$

$= 1 + 1 - 0 = 2. > 1 = S(A)$

- $0 \leq S(C|A) + S(C|B)$

  But, $0 \nleq S(A|C) + S(B|C)$

Ex:- Let,

ABC be a product of a pure state for A with an EPR state for BC.

$S(A) = 0$ since A is a pure state.

$S(B|C) < 0$ since AB is entangled.

□ Theorem 11.15

- Conditioning reduces entropy:

- Suppose ABC is a composite quantum system. Then,

$$\boxed{S(A|B,C) \leq S(A|B)}$$

Proof.

$$S(A|B,C) \leq S(A|B)$$
$$\Longrightarrow S(A,B,C) - S(B,C) \leq S(A,B) - S(B)$$
$$\Longrightarrow S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$$

which is strong subadditivity.

- Disregarding quantum systems never increases mutual information:

– Suppose ABC is a composite system. Then

$$\boxed{S(A:B) \le S(A:B,C)}$$

Proof

$$S(A:B) \le S(A:B,C)$$

$$\Rightarrow \cancel{S(A)} + S(B) - S(A,B) \le \cancel{S(A)} + S(B,C) - S(A,B,C)$$

$$\Rightarrow S(A,B,C) + S(B) \le S(A,B) + S(B,C).$$

- Quantum operations never increase mutual information.

– AB is a composite quantum system and $\mathcal{E}$ is a trace-preserving quantum operation on system B. Let $S(A:B)$ be the mutual information b/w systems A & B before $\mathcal{E}$ is applied to system B, and $S(A':B')$ be the mutual information after $\mathcal{E}$ is applied to system B. Then

$$\boxed{S(A':B') \le S(A,B)}$$

Proof.

The action of $\mathcal{E}$ on B may be simulated by introducing a 3^{rd} system C, initially in a pure state $|0\rangle$, and a unitary interaction U b/w B and C.

i.e.,
The action of $\mathcal{E}$ on B is equivalent to the action of U followed by disregarding system C.

" ' " denote the state of the systems after U has acted.

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$$

$$\therefore \quad S(A:B) = S(A) + S(B) - S(A,B)$$

$$S(A:B,C) = S(A) + S(B,C) - S(A,B,C)$$

$$= S(A) + \left[S(B) \overset{?}{+} S(C)\right] - \left[S(A,B) + S(C)\right]$$

Q:

$$= S(A) + S(B) + \cancel{S(C)} - S(A,B) - \cancel{S(C)}$$

$$= S(A) + S(B) - S(A,B) = S(A:B)$$

$$\rightarrow \quad S(A:B,C) = S(A:B)$$

$$S(\rho) = S(U\rho U^{\dagger})$$

$$\therefore \quad S(B',C') = S(B,C) \quad \& \quad S(A',B',C') = S(A,B,C)$$

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

$$= S(A) + S(B,C) - S(A,B,C) = S(A:B,C)$$

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

Discarding systems cannot increase mutual information

$$\Longrightarrow S(A':B') \leq S(A':B',C')$$

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

$$\Longrightarrow \underline{\underline{S(A':B') \leq S(A,B)}}.$$

- Shannon mutual information is not subadditive

⇒ Quantum mutual information is not subadditive.

Theorem 11.16 → **Subadditivity of the conditional entropy**

Let ABCD be a composite of 4 quantum systems. Then the conditional entropy is jointly subadditive in the 1st and 2nd entries:

$$\boxed{S(A,B|C,D) \leq S(A|C) + S(B|D)}$$

Let ABC be a composite of 3 quantum systems. Then the conditional entropy is subadditive in each of the 1st and 2nd entries:

$$\boxed{\begin{aligned} S(A,B|C) &\leq S(A|C) + S(B|C) \\ S(A|B,C) &\leq S(A|B) + S(A|C) \end{aligned}}$$

Proof. By strong subadditivity,

$$S(A,B,C) + S(B) \leq S(A,B) + S(B,C)$$

$$S(\underset{①}{A},\underset{②}{B},C,\underset{③}{D}) + S(C) \leq S(A,C) + S(B,C,D)$$

Adding $S(D)$ to each side,

$$S(A,B,C,D)+S(C)+S(D) \le S(A,C)+\underbrace{S(B,C,D)+S(D)}$$

By strong subadditivity,

$$S(A,B,C)+S(B) \le S(A,B)+S(B,C)$$

$$S(B,C,D)+S(D) \le S(B,D)+S(C,D).$$

$$S(A,B,C,D)+S(C)+S(D) \le S(A,C)+S(B,D)+S(C,D)$$

Note that, $S(A|B)=S(A,B)-S(B)$

$$S(A,B|C,D) = S(A,B,C,D)-S(C,D)$$

$$S(A|C) = S(A,C)-S(C)$$

$$S(B|D) = S(B,D)-S(D)$$

$$S(A,B,C,D)-S(C,D) \le S(A,C)-S(C)+S(B,D)-S(D)$$

$$S(A,B|C,D) \le S(A|C)+S(B|D)$$

$$S(A,B|C) \le S(A|C) + S(B|C)$$

$$S(A,B,C) - \cancel{S(C)} \le S(A,C) - \cancel{S(C)} + S(B,C) - S(C)$$

$$S(A,B,C) + S(C) \le S(A,C) + S(B,C)$$

which is the strong subadditivity.

$$S(A|B,C) \le S(A|B) + S(A|C)$$

$$S(A,B,C) - S(B,C) \le S(A,B) - S(B) + S(A,C) - S(C)$$

$$S(A,B,C) + S(B) + S(C) \le S(A,B) + S(B,C) + S(A,C)$$

which is required to prove!

$$\left.\begin{array}{l} S(A) + S(B) \le S(A,C) + S(B,C) \\ S(B) + S(C) \le S(A,B) + S(A,C) \end{array}\right\}.$$

and $S(C) > S(A,C)$ & $S(B) > S(A,B)$ cannot be true simultaneously.

$\therefore$ $S(C) \le S(A,C)$ [or] $S(B) \le S(A,B)$

when $S(C) \le S(A,C)$,

$$S(A,B,C) + S(B) \le S(A,B) + S(B,C)$$

$$S(A,B,C) + S(B) + S(C) \le S(A,B) + S(B,C) + S(A,C)$$

Theorem 11.17 → Monotonicity of the relative entropy

Proof

Let ρ^{AB} and σ^{AB} be any 2 density matrices of a composite system AB. Then,

$$\boxed{S(\rho^{A}\|\sigma^{A}) \leq S(\rho^{AB}\|\sigma^{AB})}$$