Projections onto $*$-subalgebras and convexity inequalities

<u>Example</u>. $X \longmapsto \mathcal{E}(A) := \sum_{j=1}^{N} w_j U_j A U_j^*$

U_j unitary, $\sum_{j=1}^{N} w_j = 1$ with $w_j > 0$

<u>Example</u> (Simplest example of $*$-subalgebra)

$$\mathcal{A} = \left\{ A \in M_2(\mathbb{C}) : A = \begin{pmatrix} z & w \\ w & z \end{pmatrix},\ z, w \in \mathbb{C} \right\}$$

$\mathcal{A}$ is a unital $*$-subalgebra of $M_2(\mathbb{C})$

Moreover, we see that $\begin{pmatrix} x & y \\ y & x \end{pmatrix}\begin{pmatrix} z & w \\ w & z \end{pmatrix} = \begin{pmatrix} xz+yw & xw+yz \\ yz+xw & yw+xz \end{pmatrix}$

$$= \begin{pmatrix} z & w \\ w & z \end{pmatrix}\begin{pmatrix} x & y \\ y & x \end{pmatrix}$$

Thus $\mathcal{A}$ is in fact a commutative subalgebra of $M_2(\mathbb{C})$. $\square$

<u>Example</u>. Denote $\mathcal{A}$ as above, let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which is both self-adjoint and unitary.

Denote $E_{\mathcal{A}}(A) := \frac{1}{2}(A + XAX^*)$

- $E_{\mathcal{A}}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{2}\begin{pmatrix} a+d & b+c \\ b+c & a+d \end{pmatrix} \in \mathcal{A}$

- Consider $E_{\mathcal{A}}(A)$ and $(id - E_{\mathcal{A}})(A)$

$$E_{\mathcal{A}}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{a+d}{2} & \frac{b+c}{2} \\ \frac{b+c}{2} & \frac{a+d}{2} \end{pmatrix} \quad (id - E_{\mathcal{A}})\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{a-d}{2} & \frac{b-c}{2} \\ \frac{c-b}{2} & \frac{d-a}{2} \end{pmatrix}$$

$$\mathrm{Tr}\left([E_{\mathcal{A}}(A)]^* [(id - E_{\mathcal{A}})(A)] \right) = \mathrm{Tr}\begin{pmatrix} \frac{(\bar{a}+\bar{d})(a-d)}{2} & * \\ * & \frac{(\bar{a}+\bar{d})(d-a)}{2} \end{pmatrix} = 0$$

That is, $E_{\mathcal{A}}(A)$ and $(\mathrm{id}-E_{\mathcal{A}})(A)$ are orthogonal w.r.t. the Hilbert-Schmidt inner product.

Moreover, $E_{\mathcal{A}}^2(A) = E_{\mathcal{A}}\left(\frac{1}{2}A + \frac{1}{2}XAX^*\right) = \frac{1}{2}XAX^* + \frac{1}{2}A + \frac{1}{2}XAX^* + \frac{1}{2}A = E_{\mathcal{A}}(A)$

We have $E_{\mathcal{A}}(A)$ is the orthogonal projection of A onto $\mathcal{A}$.

By operator Jensen inequality $\left(\frac{1}{2}X^*X + \frac{1}{2}I = \frac{1}{2}I + \frac{1}{2}I = I\right)$, for any convex function f, we have

$$E_{\mathcal{A}}[f(A)] = \frac{f(A) + Xf(A)X^*}{2} \geq f\left(\frac{A+XAX^*}{2}\right) = f(E_{\mathcal{A}}[A])$$

$\square$

Example. $(A,B) \longmapsto H(A\|B) = \mathrm{Tr}(A\log A - A\log B)$

- Recall that this map is jointly convex on $\mathbb{H}_n^{>0} \times \mathbb{H}_n^{>0}$.
- Also, we can easily see that $H(A\|B)$ is unitary invariant.

Thus, for $n=2$. Let $\mathcal{A} \subseteq M_2(\mathbb{C})$ be the subalgebra defined above, we have $H(A\|B) = \frac{1}{2}\left(H(A\|B) + H(A\|B)\right)$

$$\xrightarrow[\text{invariant}]{\text{unitary}} \frac{1}{2}\left(H(A\|B) + H(XAX^*\|XBX^*)\right)$$

$$\underset{\text{joint convexity}}{\geq} H\left(\frac{A+XAX^*}{2}\middle\|\frac{B+XBX^*}{2}\right) = H\left(E_{\mathcal{A}}[A]\middle\|E_{\mathcal{A}}[B]\right).$$

We have the data-processing time inequality

$$H(E_{\mathcal{A}}[A]\|E_{\mathcal{A}}[B]) \leq H(A\|B).$$

Rmk. The notation $E_{\mathcal{A}}$ is closely analog to the operation of conditional expectation in classical prob. theory.

$(\Omega, \mathcal{F}, \mu)$ probability space

$\cup\!|$

$\mathcal{S}$ a sigma-subalgebra

$\Longrightarrow L^2(\Omega, \mathcal{S}, \mu|_{\mathcal{S}}) \overset{\text{closed}}{\subseteq} L^2(\Omega, \mathcal{F}, \mu)$

X : bounded random variable on $(\Omega, \mathcal{F}, \mu)$

conditional expectation $E(X|\mathcal{S}) \in L^2(\Omega, \mathcal{S}, \mu|_{\mathcal{S}})$

$X \mapsto E(X|\mathcal{S})$ can be viewed as the orthogonal projection from $L^2(\Omega, \mathcal{F}, \mu)$ onto $L^2(\Omega, \mathcal{S}, \mu|_{\mathcal{S}})$

In fact, the bounded measurable functions on $(\Omega, \mathcal{F}, \mu)$ form a commutative $*$-algebra, of which the bounded measurable functions on $(\Omega, \mathcal{S}, \mu|_{\mathcal{S}})$ form a commutative $*$-subalgebra.

Def. (commutant) $\mathcal{A}$ subset of $M_n(\mathbb{C})$.

$\mathcal{A}'$, the commutant of $\mathcal{A}$; is given by

$$\mathcal{A}' := \{ B \in M_n(\mathbb{C}) : BA = AB \text{ for all } A \in \mathcal{A} \}$$

It is easy to see that:

- For any <u>set</u> $\mathcal{A}$, $\mathcal{A}'$ must be a subalgebra of $M_n(\mathbb{C})$
- If we additionally assume that $\mathcal{A}$ is closed under $A \mapsto A^*$, then $\mathcal{A}'$ is a $*$-subalgebra of $M_n(\mathbb{C})$.

(In part., if $\mathcal{A}$ is already a $*$-subalg. of $M_n(\mathbb{C})$, then so is $\mathcal{A}'$)

Thm. (von Neumann double commutant thm.)

For any $*$-subalg. $\mathcal{A}$ of $M_n(\mathbb{C})$, we have $\mathcal{A}'' = \mathcal{A}$.

Proof ① We first show that for any $*$-subalg. $\mathcal{A}$, and any $B \in \mathcal{A}''$, $v \in \mathbb{C}^n$, $\exists\, A \in \mathcal{A}$ such that $Av = Bv$.

If this has already been established, we apply this to

$$\mathcal{M} := \left\{ \begin{pmatrix} A & & \\ & A & \\ & & \ddots_{A} \end{pmatrix} = A \otimes I_n : A \in \mathcal{A} \right\} \underset{*\text{-subalg.}}{\subseteq} M_{n^2}(\mathbb{C}), \text{ then}$$

(easy to verify)

for any $\tilde{B} \in \mathcal{M}''$, $\exists\, A \in \mathcal{A}$ such that

$$\tilde{B} v \overset{(*)}{=} (A \otimes I_n) v \quad \text{for } v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{C}^{n^2} \text{ where}$$

$\{v_1, \cdots, v_n\}$ is a basis of $\mathbb{C}^n$.

Now we compute the structure of $\mathcal{M}''$. It is easy to see that

$$\mathcal{M}' = \left\{ \begin{pmatrix} X & & \\ & \ddots & \\ & & X \end{pmatrix} = X \otimes I_n : X \in \mathcal{A}' \right\}, \text{ therefore}$$

$$\mathcal{M}'' = \left\{ \begin{pmatrix} X & & \\ & \ddots & \\ & & X \end{pmatrix} = X \otimes I_n : X \in \underset{\mathcal{A}''}{(\mathcal{A}')'} \right\}. \text{ Thus w.l.o.g. we let}$$

$$\tilde{B} = \begin{pmatrix} B & & \\ & \ddots & \\ & & B \end{pmatrix} = B \otimes I_n \text{ for } B \in \mathcal{A}'', \text{ then } (*) \text{ translates to}$$

$Bv_i = Av_i$ for $i = 1, \cdots, n$ $\Rightarrow B = A \Rightarrow$ We have proved that for any $B \in \mathcal{A}''$, $\exists\, A \in \mathcal{A}$ such that $B = A \Rightarrow \mathcal{A}'' \subseteq \mathcal{A}$.

But $\mathcal{A} \subseteq \mathcal{A}''$ holds trivially, thus $\mathcal{A} = \mathcal{A}''$. □

② It suffices to prove the claim above.

Fix any ~~state~~ vector $v \in \mathbb{C}^n$, let $V = \{Av : A \in \mathcal{A}\} = \cancel{A(v)}\ \mathcal{A}v$ the subspace of $\mathbb{C}^n$ and consider P_V

<u>Claim</u>. $P_V \in \mathcal{A}'$. That is because $P_V A P_V = A P_V$ for any $A \in \mathcal{A}$. (V is $\mathcal{A}$-invariant)

$$\xRightarrow{\text{taking adjoint}} \quad P_V A^* = P_V A^* P_V \quad \text{for any } A \in \mathcal{A}$$

$$\xRightarrow{\mathcal{A} \text{ is a *-subalg.}} \quad P_V A = P_V A P_V \quad \text{for any } A \in \mathcal{A}$$

$$\xRightarrow{\text{together with } P_V A P_V = A P_V} \quad A P_V = P_V A P_V = P_V A \quad (\forall A \in \mathcal{A}) \Rightarrow P_V \in \mathcal{A}'$$

Thus, $\forall B \in \mathcal{A}''$, $BP_V = P_V B \Rightarrow V$ is $\mathcal{A}''$-invariant

In particular, $\underset{\mathcal{A}''}{B}\underset{V\ (\mathcal{A} \text{ is unital})}{v} \in V$ (by V is $\mathcal{A}''$-invariant)

$$\xRightarrow{\text{by def. of } V} \quad \exists A \in \mathcal{A} \text{ such that } Bv = Av$$

$\square$

<u>Rmk</u>. In the standard inf.-dim. operator theory, the proof of the vN double commutant theorem is essentially the same. The relevant difference lies in the fact that the subspace V are <u>not</u> always <u>closed</u> in inf.-dim. case. We have to replace V by $V = \overline{\{Av : A \in \mathcal{A}\}}$ and we can also prove $\forall B \in \mathcal{A}''$ $Bv \in \overline{\{Av : A \in \mathcal{A}\}}$. Thus one conclude $\underline{\mathcal{A}'' = \overline{\mathcal{A}}^{w.o.T.}}$ where $\overline{}^{w.o.T.}$ denotes taking the weak operator closure of $\mathcal{A}$.

Example. $\mathcal{A}=\left\{\begin{pmatrix} z & w\\ w & z\end{pmatrix} : z,w\in\mathbb{C}\right\} \underset{*\text{-subalg.}}{\subset} M_2(\mathbb{C})$

$\mathcal{A}$ happens to be commutative $\Longrightarrow$ $\mathcal{A}\subseteq\mathcal{A}'$ in this case

In fact, $\mathcal{A}$ is spanned by I and X (as subspace), so

$$\left(A\in\mathcal{A}' \Longleftrightarrow AX=XA \Longleftrightarrow A\in\mathcal{A}\right) \Longrightarrow \mathcal{A}=\mathcal{A}'$$

$\underset{\text{obviously}}{\Longrightarrow}$ $\mathcal{A}=\mathcal{A}''$ as vN thm. tells us.

Thm ($A|_{\mathcal{A}}$ is invertible on $\mathcal{A}$)

Let $\mathcal{A} \underset{*\text{-subalg.}}{\subset} M_n(\mathbb{C})$. $\forall A\in\mathcal{A}$, A invertible, we have $A^{-1}\in\mathcal{A}$.

(A invertible in ~~$\mathcal{A}$~~ $M_n(\mathbb{C}) \Longrightarrow A$ invertible in $\mathcal{A}$).

We need the following technical lemmas.

Lem. $\mathcal{A} \underset{*\text{-subalg.}}{\subset} M_n(\mathbb{C})$, for any $A\in\mathcal{A}$ Hermitian, let

$A=\sum_{j=1}^{m}\lambda_j P_j$ be the spectral ~~projection~~ decomposition of A for $\lambda_j\in\mathbb{R}$

Then each of P_j belongs to $\mathcal{A}$. Moreover, each $A\in\mathcal{A}$ can be written as a lin. comb. of at most four unitaries, ~~with~~ each of them belongs to $\mathcal{A}$.

$\operatorname{diag}(\lambda_i-\lambda_j)_{1\le j\le n}$

↑eigenbasis ① $\mathcal{A}$ is an alg.

Proof of Lem. $P_j=\prod_{i\in\{1,\dots,n\}\setminus\{j\}}\frac{1}{\lambda_i-\lambda_j}\underline{(\lambda_i I-A)}\in\mathcal{A}$.

② $A\in\mathcal{A}$

For A self-adjoint and contractive, $\lambda_j\in[-1,1]\Longrightarrow\lambda_j=\cos\theta_j$ for $\theta_j\in[0,\pi]$

$$\Longrightarrow A=\sum_{j=1}^{m}\lambda_j P_j=\sum_{j=1}^{m}\frac{1}{2}\left(e^{i\theta_j}+e^{-i\theta_j}\right)P_j=\frac{1}{2}\Bigg(\underbrace{\sum_{j=1}^{m}e^{i\theta_j}P_j}_{\substack{\text{unitary}\\ \in\mathcal{A}}}+\underbrace{\sum_{j=1}^{m}e^{-i\theta_j}P_j}_{\substack{\text{unitary}\\ \in\mathcal{A}}}\Bigg)$$

Thus it holds for self-adjoint contraction.

For general $A \in \mathcal{A}$, we write $A = \underbrace{\frac{1}{2}(A+A^*)}_{\text{self-adjoint}} + \frac{1}{2i}[i(A-A^*)]$

It readily follows by a scaling of these self-adjoint matrices. □

Lem. $\underset{*\text{-subalg.}}{\mathcal{A} \subseteq} M_n(\mathbb{C})$, then $\forall A \in M_n(\mathbb{C})$,

$A \in \mathcal{A} \iff A = UAU^*$ for ~~some~~ all ~~unitary~~ matrix $U \in \mathcal{A}'$.

Proof. observe: $A = UAU^*$ iff $UA = AU$ for all unitary U

$\Rightarrow$ $A = UAU^*$ for all $U \in \mathcal{A}'$ ~~translates into~~ $\Longrightarrow$ A commutes with every unitary matrix in $\mathcal{A}'$

$\Rightarrow$ By writing any matrix in $\mathcal{A}'$ as linear ~~(by writing U as linear comb. of unitaries in $\mathcal{A}'$)~~ sum of unitaries according to the prev. lem., A commutes with every matrix in $\mathcal{A}'$ $\Longrightarrow$ By vN double commutant thm., $A \in \mathcal{A}''$

$\Rightarrow A \in \mathcal{A}$ □

Rmk. It is useful to think:

All $*$-subalg. of $M_n(\mathbb{C})$ contain "plenty of projections and plenty of unitaries" according to the prev. lemma.

There is in fact another important ~~think of~~ sense in which $*$-subalg. of $M_n(\mathbb{C})$ are rich in unitaries:

Lem. $\underset{*\text{-sub alg.}}{\mathcal{A} \subseteq} M_n(\mathbb{C})$, $B \in H_n^{>0} \cap \mathcal{A}$, then $B^{-1} \in \mathcal{A}$.

Proof. $\|I - \|B\|^{-1}B\| < 1 \Longrightarrow (\|B\|^{-1}B)^{-1} = \sum_{n=0}^{\infty} \underbrace{(I - \|B\|^{-1}B)^n}_{\in \mathcal{A}}$

$\Rightarrow \|B\| \cdot B^{-1} \in \mathcal{A} \Rightarrow B^{-1} \in \mathcal{A}$. $\square$

Rmk. $\forall \varepsilon > 0$, $A \in \mathcal{A} \Rightarrow A(A^*A + \varepsilon I)^{-1/2} \in \mathcal{A}$

$\xrightarrow[\varepsilon \to 0]{}$ " $A|A|^{-1} \in \mathcal{A}$ ". That is, if $A = U|A|$ is the polar-decom of A, then both U and $|A|$ belongs to $\mathcal{A}$.

We next provide ~~a~~ the proof of the theorem of the invertibility of A in $\mathcal{A}$.

Proof of the theorem.

Let $A \in M_n(\mathbb{C})$ be invertible, $A = U|A|$ be the polar decomposition of A. Then $A^{-1} = |A|^{-1} U^*$.
By the remark above, since $A \in \mathcal{A}$, we have $U, |A| \in \mathcal{A}$.
Since $\mathcal{A}$ is a $*$-subalgebra, we have $U^* \in \mathcal{A}$. It remains to show that $|A|^{-1}$ is in $\mathcal{A}$ as well, which immediately follows from the above lemma $\square$.
(the inverse of positive definite matrix is still in the $*$-sub alg.).

Def. We call the orthogonal projection $E_{\mathcal{A}}$ of $M_n(\mathbb{C})$ onto $\mathcal{A}$ the <u>conditional expectation given $\mathcal{A}$</u>.

Example.

- Let $\{u_1, \dots, u_n\}$ is an O.N. basis of $\mathbb{C}^n$
- Let $\mathcal{A}$ be the sub alg. of $M_n(\mathbb{C})$ defined as

$$\mathcal{A} = \left\{ \sum_{j=1}^n a_j u_j u_j^* \; : \; a_j \in \mathbb{C} \right\} \text{ (diagonal subalg. under } \{u_j\}_{j=1}^n \text{)}.$$

- For $B \in M_n(\mathbb{C})$, $\widetilde{B} := \sum_{j=1}^n \langle u_j, B u_j \rangle u_j u_j^* \in \mathcal{A}$

↳ conjugate linear on the left

- For any $A \in \mathcal{A}$, we compute (let $A = \sum_{j=1}^n a_j u_j u_j^*$)

$$\begin{aligned}
\mathrm{Tr}(A(B-\widetilde{B})) &= \sum_{j=1}^n \langle u_j, A(B-\widetilde{B}) u_j \rangle \\
&= \sum_{j=1}^n \langle u_j, AB u_j \rangle - \sum_{j=1}^n \underbrace{\langle u_j, A u_j \rangle}_{\parallel} \langle u_j, B u_j \rangle \\
&= \sum_{j=1}^n \langle A^* u_j, B u_j \rangle - \sum_{j=1}^n a_j \langle u_j, B u_j \rangle \\
&= \sum_{j=1}^n \langle \bar{a}_j u_j, B u_j \rangle - \sum_{j=1}^n a_j \langle u_j, B u_j \rangle \\
&= \sum_{j=1}^n a_j \langle u_j, B u_j \rangle - \sum_{j=1}^n a_j \langle u_j, B u_j \rangle = 0.
\end{aligned}$$

Thus $A^* \perp B - \widetilde{B}$ w.r.t. the Hilbert–Schmidt inner prod. for any $A \in \mathcal{A}$, that is, $B - \underset{\mathcal{A}}{\underset{\cap}{\widetilde{B}}} \perp \mathcal{A}$. Thus we have (by defn.)

$$E_{\mathcal{A}}(B) = \widetilde{B} = \sum_{j=1}^n \langle u_j, B u_j \rangle u_j u_j^*.$$

(the explicit formula of conditional expectation on the diagonal subalgebra)

Recall. Thm. (Projection) Let K be a closed convex set in a Hilbert space. Then K contains a unique element of minimal norm, that is, $\exists! v \in K$ such that $\|v\| = \inf_{w \in K} \|w\|$.

Proof. Standard textbook proof in functional analysis. $\square$

Rmk. Also quite useful in finite-dimensional case.

$\star$ Thm. For any $A \in M_n(\mathbb{C})$ and $*$-subalg. $\mathcal{A}$ of $M_n(\mathbb{C})$, let K_A denotes the closed convex hull of operators UAU^*, $U \in \mathcal{A}'$

i.e. $K_A := \overline{\mathrm{co}} \{ UAU^* : \underset{\text{unitary}}{U \in \mathcal{A}'} \}$.

Then $E_{\mathcal{A}}(A)$ is the unique element of minimal (H-S) norm in K_A. Furthermore, ① $\operatorname{Tr} E_{\mathcal{A}}(A) = \operatorname{Tr} A$ ② $A > 0 \Rightarrow E_{\mathcal{A}}(A) > 0$

③ For each $B \in \mathcal{A}$, $E_{\mathcal{A}}(BA) = B E_{\mathcal{A}}(A)$, $E_{\mathcal{A}}(AB) = E_{\mathcal{A}}(A) B$

"bimodule property of conditional expectation"

Recall. Lemma. $\underset{*\text{-sub alg.}}{\mathcal{A} \subseteq} M_n(\mathbb{C})$. $A \in \mathcal{A} \iff A = UAU^*$ for any $U \in \mathcal{A}'$

[$A = UAU^*$ for any $U \in \mathcal{A}' \Rightarrow A$ commutes with all the unitaries in $\mathcal{A}' \Rightarrow A$ commutes with all operators in $\mathcal{A}'$ $\Rightarrow A \in \mathcal{A}''$] $\overset{\text{i.e.}}{\underset{\text{vN}}{\Longrightarrow}} A \in \mathcal{A}$

↳ All the ~~matrices~~ matrices in $*$-subalg. can be written as up to 4 unitary operators.
lin. sum. of

Step 1.

Proof of the thm. $(M_n, \underset{\text{H-S}}{\langle \cdot , \cdot \rangle})$ Hilbert space

Proj. thm. $\Longrightarrow \exists! \tilde{A} \in K_A$ such that $\|\tilde{A}\| = \inf_{X \in K_A} \|X\|$.

Let $U \in \mathcal{A}'$ be unitary (by the previous lemma it must exist)

By the parallelogram law,

$$\left\| \underbrace{\frac{\tilde{A} + u\tilde{A}u^*}{2}}_{\in K_A \text{ by construct. (convex comb. of } \tilde{A} \text{ and } u\tilde{A}u)} \right\|^2 + \left\| \frac{\tilde{A} - u\tilde{A}u^*}{2} \right\|^2 = \frac{\|\tilde{A}\|^2 + \underbrace{\|u\tilde{A}u^*\|^2}_{\|\tilde{A}\|^2}}{2} = \|\tilde{A}\|^2$$

~~by construct.~~

$$\geq \|\tilde{A}\| + \left\| \frac{\tilde{A} - u\tilde{A}u^*}{2} \right\|^2$$

$\|\tilde{A}\| = \inf_{X \in K_A} \|X\|$

$$\Rightarrow \left\| \frac{\tilde{A} - u\tilde{A}u^*}{2} \right\|^2 = 0 \Rightarrow \tilde{A} = u\tilde{A}u^* \text{ for all unitary } u \in \mathcal{A}'$$

$$\underset{\text{previous lemma}}{\Longrightarrow} \tilde{A} \in \mathcal{A}'' \underset{\substack{\text{vN} \\ \text{doub. comm.}}}{\Rightarrow} \tilde{A} \in \mathcal{A}$$

Step 2. We claim that $\langle B, A - \tilde{A} \rangle = 0$ for any $B \in \mathcal{A}$

That is, $A - \tilde{A} \in \mathcal{A}^\perp$ or $\tilde{A}$ is the projection of A onto $\mathcal{A}$.

To see this, we first claim $\widetilde{AB} = \tilde{A}B$. In fact,

for any convex comb. of $\mathcal{A}'$-unitary conjugations of AB,

$$\sum_{j=1}^N w_j u_j (A \underbrace{B}_{\in \mathcal{A}}) \underbrace{u_j^*}_{\in \mathcal{A}'} = \left(\sum_{j=1}^N w_j u_j A u_j^* \right) \cdot B$$

$$\Rightarrow \widetilde{AB} = \tilde{A}B$$

On the other hand since unitary conjugation is trace-invariant, thus any matrix in K_A (K_{AB}) has the same trace as A (AB) i.e.

$$\mathrm{Tr}[\widetilde{AB}] = \mathrm{Tr}(AB), \quad \mathrm{Tr}[\tilde{A}] = \mathrm{Tr}(A)$$

$$\Rightarrow \underbrace{\mathrm{Tr}\left(B^*(A - \tilde{A}) \right)}_{\langle B, A - \tilde{A} \rangle =} = \mathrm{Tr}\left(B^*A - B^*\tilde{A} \right) = \mathrm{Tr}(\widetilde{B^*A} - B^*\tilde{A}) = 0$$

Step 3. Recall that we ~~have~~ define $E_{\mathcal{A}}(A)$ as the projection of A onto $\mathcal{A}$ as the lin. subspace of $M_n(\mathbb{C})$. Thus by Step 2, we have $\tilde{A} = E_{\mathcal{A}}(A)$ (well-defined by the uniqueness of $\tilde{A}$). Thus, ~~for $B \in \mathcal{A}$~~.

① It follows readily that $E_{\mathcal{A}}$ is trace-preserving
$\mathrm{Tr}\, E_{\mathcal{A}}(A) = \mathrm{Tr}\,\tilde{A} = \mathrm{Tr}\, A$.

② For any $B \in \mathcal{A}'$

- $E_{\mathcal{A}}(AB) = \widetilde{AB} = \tilde{A}B = E_{\mathcal{A}}(A) \cdot B$
- $E_{\mathcal{A}}(BA) = \widetilde{BA} = B\tilde{A} = B \cdot E_{\mathcal{A}}(A)$

(bimodule property)

③ For any $A > 0$, $UAU^* > 0$ for any U unitary. Thus

$E_A(\mathcal{A}) \in K_A = \overline{\mathrm{Co}\{UAU^* : \underset{\text{unitary}}{U \in \mathcal{A}'}\}}$ must be positive. □

Rmk. In finite dimensional case, $E_{\mathcal{A}}$ can be written as

$E_{\mathcal{A}}(A) = \sum_{j=1}^{N} w_j U_j A U_j^*$ " ~~weighted~~ convex comb. of unitary conjugations of A"

This is a very useful argument in f.d. cases. This theorem also provides us with more characteristic information about cond. exp., such as

- "bimodule property" $E_{\mathcal{A}}(BAC) = B\, E_{\mathcal{A}}(A)\, C$ for any $B, C \in \mathcal{A}$, $A \in M_n(\mathbb{C})$
- "trace-preserving" $\mathrm{Tr}\, E_{\mathcal{A}}(A) = \mathrm{Tr}\, A$
- "projection formulation" $E_{\mathcal{A}}(A) = \inf_{X \in K_A} \|X\|$

with $K_A = \overline{\mathrm{Co}\{UAU^* : U \text{ unitary}, U \in \mathcal{A}'\}}$.

Example "the diagonal subalgebra" $\mathcal{A} = \{\sum_{j=1}^{n} a_j u_j u_j^*,\ a_j \in \mathbb{C}\}$ $\subseteq M_n(\mathbb{C})$ $*$-subalg.

For $k = 1, \dots, n$ define $U_k = \sum_{j=1}^{n} e^{i2\pi jk/n} u_j u_j^*$

$B \in M_n(\mathbb{C})$, then $U_k B U_k^* = \sum_{l,m=1}^{n} \langle u_m, B u_l \rangle e^{\frac{i2\pi(l-m)k}{n}} u_m u_l^*$

$$\Rightarrow \frac{1}{n} \sum_{k=1}^{n} U_k B U_k^* = \sum_{l,m=1}^{n} \langle u_m, B u_l \rangle \underbrace{\left(\frac{1}{n} \sum_{k=1}^{n} e^{\frac{i2\pi(l-m)k}{n}} \right)}_{= \delta_{ml} \text{ (discrete Fourier transform)}} u_m u_l^*$$

$$= \sum_{m=1}^{n} \langle u_m, B u_m \rangle u_m u_m^* = E_{\mathcal{A}}(B)$$

That is, "taking the diagonal part" is an average of n unitary conjugations of B. $\square$

Next, we provide an important convexity inequality of cond. exp.

Thm. Let f be any operator convex function. Then for any $*$-subalgebra $\mathcal{A}$ of $M_n(\mathbb{C})$, $f(E_{\mathcal{A}}(A)) \leq E_{\mathcal{A}}(f(A))$.

Proof.

Note that $f(E_{\mathcal{A}}(A)) - E_{\mathcal{A}}(f(A)) \in \mathcal{A}$ is self-adjoint by functional calculus, by the previous lem., all the spectral projections of $f(E_{\mathcal{A}}(A)) - E_{\mathcal{A}}(f(A))$ is in $\mathcal{A}$. Then it suffices to show ~~reduces to showing~~ that for any orthogonal projection $P \in \mathcal{A}$, we have

$$\mathrm{Tr}[P f(E_{\mathcal{A}}(A))] \leq \mathrm{Tr}[P E_{\mathcal{A}}(f(A))]$$

But since we have $P \in \mathcal{A}$, $\mathrm{Tr}[P E_{\mathcal{A}}(f(A))] \xrightarrow[\text{property}]{\text{bimodule}} \mathrm{Tr}[E_{\mathcal{A}}(P f(A))]$

$= \mathrm{Tr}(P f(A))$

We write $E_{\mathcal{A}}(A) = \cancel{\lim} \sum_{j=1}^{N} p_j U_j A U_j^*$ for $\underset{\in \mathcal{A}'}{U_j}$ unitary, $\sum_{j=1}^{N} p_j = 1$, $p_j > 0$

By the operator convexity of f and the operator Jensen ineq.

$$f(E_{\mathcal{A}}(A)) \leq \sum_{j=1}^{N} p_j U_j f(A) U_j^* \left(\cancel{= \sum_{j=1}^{N} p_j f(U_j A U_j^*)} \right)$$

$$\Rightarrow \mathrm{Tr}[P f(E_{\mathcal{A}}(A))] \leq \cancel{\sum_{j=1}^{N} p_j \mathrm{Tr}[P f(U_j A U_j^*)]}$$

$$\sum_{j=1}^{N} p_j \mathrm{Tr}[\underset{\mathcal{A}}{P} \underset{\mathcal{A}'}{U_j} f(A) U_j^*]$$

$$= \sum_{j=1}^{N} p_j \mathrm{Tr}[U_j (P f(A)) U_j^*] = \sum_{j=1}^{N} p_j \mathrm{Tr}[P f(A) \underbrace{U_j^* U_j}_{= I}]$$

$$= \sum_{j=1}^{N} p_j \mathrm{Tr}[P f(A)] = \mathrm{Tr}[P f(A)]$$

□

<u>Corollary</u> As we have shown in "the basic properties of cond. exp.",

- $A \geq 0 \Rightarrow E_{\mathcal{A}}(A) \geq 0$, $\mathrm{Tr}\, E_{\mathcal{A}}(A) = \mathrm{Tr}\, A$

  Thus if $\rho \in \mathcal{D}(\mathbb{C}^n)$ is a n-dim. density mat., then so is $E_{\mathcal{A}}(\rho)$. $(\rho \in \mathcal{D}(\mathbb{C}^n) \Rightarrow E_{\mathcal{A}}(\rho) \in \mathcal{D}(\mathbb{C}^n))$

- For any $\mathcal{A} \underset{*\text{-subalg.}}{\subseteq} M_n(\mathbb{C})$, $H(\rho) \leq H(E_{\mathcal{A}}(\rho))$

  $H(\rho) := -\mathrm{Tr}(\rho \log \rho)$.

<u>Proof</u>. Since $x \mapsto x \log x$ is convex, we have

$$E_{\mathcal{A}}(\rho) \log[E_{\mathcal{A}}(\rho)] \leq E_{\mathcal{A}}(\rho \log \rho)$$

□

$\Rightarrow -H(E_{\mathcal{A}}(\rho)) = \mathrm{Tr}(E_{\mathcal{A}}(\rho)[\log E_{\mathcal{A}}(\rho)]) \leq \mathrm{Tr}\, E_{\mathcal{A}}(\rho \log \rho) = -H(\rho) \Rightarrow H(\rho) \leq H(E_{\mathcal{A}}(\rho))$

Example (Pinching)

$A \in \mathbb{H}_n$. $A = \sum_{j=1}^{k} \lambda_j P_j$, $\sum_{j=1}^{k} P_j = I$

Let $\mathcal{M}_A = \{A\}'$ (commutant of A), and $\mathcal{M}_A \underset{*\text{-sub alg.}}{\subseteq} M_n(\mathbb{C})$

We denote $E_A := E_{\mathcal{M}_A}$.

Claim. $E_A(B) = \sum_{j=1}^{k} P_j B P_j$.

Proof.

- RHS $\in \mathcal{M}_A$. That is because

$$\left(\sum_{j=1}^{k} P_j B P_j\right) A = \sum_{j=1}^{k} \underbrace{\lambda_j P_j}_{= AP_j} B P_j = A\left(\sum_{j=1}^{k} P_j B P_j\right)$$

$$\Rightarrow \sum_{j=1}^{k} P_j B P_j \in \{A\}' =: \mathcal{M}_A.$$

- Recall $P_j = \prod_{i \neq j} \frac{1}{\lambda_i - \lambda_j} (\lambda_i I - A)^{(\Delta)}$ is a polynomial of A,

we have $P_j A = A P_j$ and thus $P_j \in \{A\}' =: \mathcal{M}_A$.

We take arbitrary $C \in \mathcal{M}_A$, by (Δ) we have $CP_j = P_j C$,

thus:

$$\left(E_A(B)\right) C = \sum_{j=1}^{k} P_j B P_j C = \sum_{j=1}^{k} P_j B C P_j$$

$$\Rightarrow \mathrm{Tr}\left(\left[(id - E_A)(B)\right] C\right) = \mathrm{Tr}(BC) - \mathrm{Tr}\left(\sum_{j=1}^{k} P_j B C P_j\right)$$

$$= \mathrm{Tr}(BC) - \mathrm{Tr}\left(\cancel{\left(\sum_{j=1}^{k} P_j B P_j\right) BC}\right) = \mathrm{Tr}\left(BC \underbrace{\left(\sum_{j=1}^{k} P_j\right)}_{= I}\right) = \mathrm{Tr}\, BC - \mathrm{Tr}\, BC = 0$$

$\Rightarrow E_A(B)$ is indeed the orth. proj. onto $\mathcal{M}_A$ of B. $\square$

Rmk. In fact we can use this to deduce $\begin{cases} \text{Sherman-Davis ineq.} \\ \text{Operator Jensen ineq.} \end{cases}$

For instance, in the "pinching" example, by the convexity theorem we have for any oper. conv. funct. f,

$$f(E_A(B)) \leq E_A f(B) \quad \text{i.e.}$$

$$\underline{f\left(\sum_{j=1}^{k} P_j B P_j\right) \leqslant f(B)}.$$