Eötvös Loránd Tudományegyetem
Természettudományi Kar

Kvantum Rényi-divergenciák tulajdonságai és alkalmazásaik

Szakdolgozat

Simon Richárd

Matematika BSc
Alkalmazott matematikus szakirány

Témavezető:

Dr. Mosonyi Milán
egyetemi docens
BME Analízis Tanszék

Belső konzulens:

Dr. Frenkel Péter Ernő
adjunktus
ELTE Algebra és Számelmélet Tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2018

Tartalomjegyzék

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek az érdekes témát, és hogy mindig fordulhattam hozzá kérdéseimmel. Továbbá szeretném megköszönni családomnak és barátaimnak hogy egyetemi éveim alatt támogattak.

1. fejezet

Bevezetés

Rényi Alfréd 1960-ban megjelent cikkében definiálta a később róla elnevezett Rényi-divergenciákat. Ezek azóta intenzíven kutatott mennyiségek, köszönhetően számos érdekes tulajdonságuknak és alkalmazhatóságuknak a klasszikus és a kvantum-információelméletben. Ebben a szakdolgozatban megvizsgáljuk a kvantum-információ-elmélet alapfogalmait, majd egy kommunikációs probléma kapcsán bevezetjük a **Rényi-divergenciákat**, amelyek állapotok megkülönböztethetőségét formalizálják. Megvizsgáljuk néhány tulajdonságukat, belátunk egy, a kvantum-hipotézisvizsgálatban fontos szerepet játszó monotonitási tulajdonságot, majd egy állapotklónozásbeli alkalmazást mutatunk meg. A dolgozat áttekintő jellegű, a bemutatott eredményekhez részletes hivatkozási listát adunk meg.

1.1. Alapfogalmak

Az alapfogalmak áttekintésénél a [9] jegyzetre támaszkodunk.

Szemidefinit rendezés

1.1.1. Definíció. Legyen $\mathscr{H}$ véges dimenziós Hilbert tér. Azt mondjuk, hogy az $A \in \mathscr{B}(\mathscr{H})$ operátor nemnegatív ($A \geq 0$) ha pozitív szemidefinit, azaz ha $\forall x \in \mathscr{H}$ $\langle Ax, x\rangle \geq 0$.

Legyenek $A, B \in \mathscr{B}(\mathscr{H})$ operátorok. Azt mondjuk, hogy $A \geq B$, ha $A - B \geq 0$.

1.1.2. Definíció (Hilbert-Schmidt skalárszorzat)**.** Legyenek $\mathscr{H}, \mathscr{K}$ véges dimenziós Hilbert-terek. Ekkor $\langle A, B\rangle_{HS} := \mathrm{Tr} A^*B,\ \ A, B \in Lin(\mathscr{H}, \mathscr{K})$ skalárszorzatot definiál $Lin(\mathscr{H}, \mathscr{K})$-n.

Megjegyzés. A fizikában és a mátrixanalízisben a skalárszorzatot gyakran az első változóban definiálják konjugáltan lineárisnak, és második változóban lineárisnak, amint azt a fenti definíció is mutatja.

1.1.3. Állítás. *A fenti formula valóban skalárszorzat $Lin(\mathscr{H}, \mathscr{K})$-n.*

Bizonyítás.

$$\langle \lambda(A_1 + A_2), B\rangle_{HS} = \mathrm{Tr}(\lambda A_1 A_2)^* B = \overline{\lambda}(\mathrm{Tr} A_1^* B + \mathrm{Tr} A_2^* B) = \overline{\lambda}\, \mathrm{Tr} A_1^* B + \overline{\lambda}\, \mathrm{Tr} A_2^* B$$
$$= \overline{\lambda}\langle A_1, B\rangle + \overline{\lambda}\langle A_2, B\rangle$$

$$\langle A, \lambda(B_1 + B_2)\rangle = \mathrm{Tr} A^*(\lambda(B_1 + B_2)) = \lambda\, \mathrm{Tr} A^*(B_1 + B_2) = \lambda\, \mathrm{Tr} A^* B_1 + \lambda\, \mathrm{Tr} A^* B_2$$
$$= \lambda\langle A, B_1\rangle + \lambda\langle A, B_2\rangle$$

Legyen $\{e_i\}_{i=1}^d$ bázis $\mathscr{H}$-ban. Ekkor $\langle A, A\rangle = \sum_{i=1}^{d} \langle e_i, A^* A e_i\rangle = \sum_{i=1}^{d} ||Ae_i||^2$ Ami nemnegatív, és pontosan akkor 0, ha $Ae_i = 0\ \forall i = 1 \ldots d$ ami ekvivalens azzal, hogy A a 0 operátor. □

Dirac-formalizmus

A következőkben bevezetjük a kvantummechanikában bevett, úgynevezett bra-ket jelölésrendszert.

1.1.4. Definíció. Legyen $\mathscr{H}$ véges dimenziós Hilbert-tér.

$\forall x \in \mathscr{H}$-ra jelölje $\langle x| \in Lin(\mathscr{H}, \mathbb{C}$ azt az operátort melyre $\forall y \in \mathscr{H}$-ra:$\langle x| : y \mapsto \langle x, y\rangle$.

$\forall x \in \mathscr{H}$-ra jelölje $|x> \in Lin(\mathbb{C},\mathscr{H})$ az $\langle x|$ operátor adjungáltját, azaz $\forall \lambda \in \mathbb{C}$: $|x\rangle : \lambda \mapsto \lambda x$

$\forall x,y \in \mathscr{H}$-ra a $\langle x| \circ |y\rangle \in Lin(\mathbb{C},\mathbb{C})$ operátort röviden $\langle x|y\rangle$-nal jelöljük.

1.1.5. Állítás. $\forall \lambda \in C < x|y >: \lambda \mapsto \lambda < x,y >$

Bizonyítás. A definíciók szerint $\langle x|y\rangle\lambda = \langle x|\lambda y = \langle x, \lambda y\rangle = \lambda \langle x,y\rangle$. □

Továbbá $\forall z \in \mathscr{H} : |y\rangle\langle x| : z \mapsto \langle x,z\rangle y$ adódik az operátorok definíciójából.

A következőkben megvizsgáljuk, hogy egy normális operátor hogyan írható fel az előbb definiált operátorok segítségével.

Spektrálfelbontás, a függvénykalkulus kiterjesztése

1.1.6. Állítás (Spektrálfelbontás 1)**.** *Legyen A normális operátor egy $\mathscr{H}$ d-dimenziós Hilbert-téren.Ekkor A a következő alakba írható:*

$A = \sum\limits_{k=1}^{d} a_k|e_k\rangle\langle e_k|$ *Ahol $e_1,...e_d$ A sajátvektorai, amik egy ortonormált bázist alkotnak $\mathscr{H}$-ban, $a_1,...,a_d$ pedig a hozzájuk tartozó sajátértékek.*

Bizonyítás. Létezik A sajátvektoraiból álló ortonormált bázis $\mathscr{H}$-ban; legyenek ezek $e_1,...,e_d$, a hozzájuk tartozó sajátértékek pedig $a_1,..,a_d$. Bármely $x \in \mathscr{H}$ vektort kifejthetünk a következő alakban: $x = \sum\limits_{i=1}^{d} \langle e_i,x\rangle e_i$, és így $Ax = \sum\limits_{i=1}^{d} \langle e_i,x\rangle Ae_i = \sum\limits_{i=1}^{d} \langle e_i,x\rangle a_i e_i = (\sum\limits_{i=1}^{d} a_i|e_i\rangle\langle e_i|)x$ □

1.1.7. Állítás (Spektrálfelbontás 2)**.** *Legyen A normális operátor egy véges dimenziós $\mathscr{H}$ Hilbert-téren. Ekkor A a következő alakba írható:$A = \sum\limits_{k=1}^{d} \lambda_k P_k$, ahol $\lambda_1,...,\lambda_d$ A különböző sajátértékei, $P_1,...,P_r$ pedig páronként ortogonális projekciók.*

Bizonyítás. Tekintsük az előző állításban látott $A = \sum\limits_{k=1}^{d} a_k|e_k\rangle\langle e_k|$ felbontást. Feltehetjük, A sajátértékei csökkenő sorrendben rendezettek, azaz $a_1 \geq a_2,..., \geq a_d$. Legyen $0 = k_0 > k_1,..., > k_d$ úgy, hogy $a_1 = ... = a_{k_1} > a_{k_2+1} = ... = a_{k_2} > a_{k_3}...$ és definiáljuk a P_j projekciókat a következőképpen:$P_j := \sum\limits_{k_{j-1}<i\leq k_j} |e_i\rangle\langle e_i|$, $\lambda_j := a_{k_j}$ ami éppen a kívánt felbontást adja. □

1.1.8. Definíció. Legyen $A \in \mathscr{B}(\mathscr{H})_{sa}$, $A = \sum\limits_{i=1}^{\dim \mathscr{H}} a_i|e_i\rangle\langle e_i|$.

Ekkor $\{A > c\} := \sum_{i:a_i>c} |e_i\rangle\langle e_i| = P^A(c, +\infty)$ és $\{A < c\} = \sum_{i:a_i<c} |e_i\rangle\langle e_i| = P^A(-\infty, c)$

$A_+ := A\{A > 0\} = \sum_{i:a_i>0} a_i|e_i\rangle\langle e_i|$

$A_- := -A\{A < 0\} = \sum_{i:a_i<0} -a_i|e_i\rangle\langle e_i|$

$|A| := \sum_{i=1}^{d} |a_i||e_i\rangle\langle e_i| = A_+ + A_-$

Függvénykalkulus operátorokon

1.1.9. Definíció. Legyen $\mathscr{H}$ véges dimenziós Hilbert-tér, és legyen A $\in \mathscr{B}(\mathscr{H})$ normális operátor. Ekkor $f(A) := \sum_{a\in spec(A)} f(a)P^A(a)$

Ahol $P^A(a)$ az A a-ra vonatkozó spektrális projekciója.

1.1.10. Állítás (A függvénykalkulus algebrai tulajdonságai)**.**

i, $(f+g)(A) = f(A)+g(A)$

ii, $(fg)(A) = f(A)g(A)$

iii, $(\lambda f)(A) = \lambda f(A)$

iv, $\bar{f}(A) = f(A)^*$*, ahol* $\bar{f} az f$ *pontonkénti konjugáltja*

v, Bármely $p(x) = \sum_{k=0}^{r} c_k x^k$ *polinomra* $p(A) = \sum_{k=0}^{r} c_k A^k$

Bizonyítás. i, Az additivitás bizonyítása:

$$(f+g)(A) = \sum_{a\in spec(A)} (f+g)(a)P^A(a) = \sum_{a\in spec(A)} f(a)P^A(a) + g(a)P^A(a)$$

$$= \sum_{a\in spec(A)} f(a)P^A(a) + \sum_{a\in spec(A)} g(a)P^A(a) = f(A) + g(A).$$

ii, A multiplikativitás bizonyítása:

$$(fg)(A) = \sum_{a\in spec(A)} (fg)(a)P^A(a) = \sum_{a\in spec(A)} f(a)g(a)P^A(a)$$

$$= \sum_{a\in spec(A)} f(a)P^A(a) * \sum_{b\in spec(A)} g(b)P^A(b) = f(A)g(A)$$

Felhasználtuk, hogy $a \neq b$ esetén $P^A(a)P^A(b) = 0$, és hogy egyenlőség esetén $f(a)g(a)P^A(a)^2 = f(a)g(a)P^(A)$, mivel $P^A(a)$ projekció.

iii, A homogenitás bizonyítása:

$$(\lambda f)(A) = \sum_{a \in spec(A)} (\lambda f)(a) P^A(a) = \sum_{a \in spec(A)} \lambda f(a) P^A(a)$$

$$= \lambda \sum_{a \in spec(A)} f(a) P^A(a) = \lambda f(A)$$

iv, A konjugált tulajdonság bizonyítása:

$$\bar{f}(A) = \sum_{a \in spec(A)} \bar{f}(a) P^A(a) = \sum_{a \in spec(A)} \bar{f}(a) P^A(a) = f(A)^*$$

v, A polinomiális tulajdonság bizonyítása:

$$p(A) = \sum_{a \in spec(A)} p(a) P^A(a) = \sum_{a \in spec(A)} \sum_{k=0}^{r} c_k a^k P^A(a)$$

$$= \sum_{k=0}^{r} c_k \sum_{a \in spec(A)} a^k P^A(a) = \sum_{k=0}^{r} c_k A^k$$

$\square$

A kvantummechanika matematikai modellje

Az alábbiakban röviden bemutatjuk a kvantummechanika matematikai modelljét, a sűrűségoperátoros tárgyalásmódra támaszkodva az állapotvektorossal szemben, mivel egy összetett rendszer részrendszerének az állapota lehet kevert akkor is, ha az egész rendszer tiszta állapotban van, így nem elég vektorállapotokkal foglalkozni.

A kvantummechanika nulladik posztulátuma:

Minden kvantumrendszernek megfeleltethető egy $\mathscr{H}$ Hilbert-tér.

Ebben a dolgozatban csak véges dimenziós Hilbert-térrel leírható kvantumrendszerekkel foglalkozunk.

1.1.11. Definíció. Egy $\rho \in Lin(\mathscr{H})$ lineáris operátort egy $\mathscr{H}$ véges dimenziós Hilbert-téren sűrűségoperátornak vagy állapotnak nevezzük, ha pozitív szemidefinit és nyoma egységnyi. A $\mathscr{H}$ Hilbert-tér $S(\mathscr{H})$ állapottere a sűrűségoperátorok halmaza:

$$S(\mathscr{H}) := \{\rho \in Lin(\mathscr{H}) : \rho \geq 0, \operatorname{Tr} \rho = 1\}$$

Megjegyzés. A $\rho \geq 0$ feltételből következik, hogy a sűrűségoperátorok sajátértékei nemnegatívak, a $\operatorname{Tr} \rho = 1$ feltételből pedig, hogy összegük 1, azaz egy $\rho \in S(\mathscr{H})$ sűrűségoperátor sajátértékei *valószínűségeloszlást alkotnak* $\dim \mathscr{H}$ ponton.

1.1.12. Definíció. Egy (véges kimenetelű) pozitív operátor értékű mérés (POVM) egy $\mathscr{H}$ Hilbert-téren $\{M_x\}_{x\in\mathscr{X}} \subset Lin(\mathscr{H})$ operátorok halmaza, ahol $\mathscr{X}$ véges halmaz, úgy, hogy $M_x \geq 0 \forall x \in \mathscr{X}$ és $\sum_{x\in\mathscr{X}} M_x = I$ Egy $\{M_x\}_{x\in\mathscr{X}}$ POVM-et projektor értékű mérésnek(PVM) nevezünk, ha minden M_x projekció, azaz $M_x^2 = M_x = M_x^*$ minden $x \in \mathscr{X}$

A kvantummechanika első posztulátuma:

Egy $\mathscr{H}$ Hilbert-térhez tartozó kvantumrendszer állapotait a $\mathscr{H}$ sűrűségoperátorai írják le. A méréseket POVM-ek írják le, amelyek a mérés lehetséges kimeneteleivel vannak indexelve. Ha a rendszer a $\rho \in S(\mathscr{H})$ állapotban van, és az $M = \{M_{x\in\mathscr{X}}\}$ POVM által leírt mérést hajtjuk végre, akkor annak valószínűsége, hogy az x kimenetelt kapjuk $P_{\rho,M}(kimenetel = x) = \operatorname{Tr} \rho M_x$

A mérések segítségével nyerünk információt a kvantumrendszerről. Ezekre tekinthetünk úgy, mint a rendszernek feltett kérdésekre, a kimenetelekre pedig mint a rendszer által adott válaszokra. A sűrűségoperátor kódolja minden előzetes információnkat a rendszerről: megadja a valószínűségét minden lehetséges kimenetelnek amit a rendszertől válaszként kaphatunk.

A fenti formulát **Born-szabálynak** hívjuk. Még bizonyításra szorul, hogy a fenti mennyiség valóban valószínűségeloszlást definiál a lehetséges mérési kimenetelek halmazán.

1.1.13. Állítás. *Legyen* $\rho \in S(\mathscr{H})$ *sűrűségoperátor, és* $\{M_x\}_{x\in\mathscr{X}}$ *POVM* $\mathscr{H}$*-n. Ekkor* $\operatorname{Tr}\rho M_x \geq 0\ \forall x \in \mathscr{H}$ *és* $\sum\limits_{x\in\mathscr{X}} \operatorname{Tr}\rho M_x = 1$*, azaz a Born szabály valószínűség-eloszlást deifinál a lehetséges mérési kimeneteleken.*

Bizonyítás. $\operatorname{Tr}\rho M_x = \operatorname{Tr}\rho^{\frac{1}{2}}\rho^{\frac{1}{2}}M_x = \operatorname{Tr}\rho^{\frac{1}{2}}M_x\rho^{\frac{1}{2}}$, ahol kihasználtuk, hogy $\rho \geq 0$, ezért létezik $\frac{1}{2}$-edik hatványa, illetve felhasználtuk a nyom ciklikusságát. Mivel $M_x \geq 0$, ezért $\rho^{\frac{1}{2}}M_x\rho^{\frac{1}{2}} \geq 0$, és így $\operatorname{Tr}\rho^{\frac{1}{2}}M_x\rho^{\frac{1}{2}} \geq 0$ Mivel $\sum_{x\in\mathscr{X}} M_x = I$, ezért $\sum\limits_{x\in\mathscr{X}} \operatorname{Tr}\rho M_x = \operatorname{Tr}\rho \sum\limits_{x\in\mathscr{X}} M_x = \operatorname{Tr}\rho I = \operatorname{Tr}\rho = 1$ □

Összetett rendszerek

Tegyük fel, hogy két kvantumrendszerünk van, $\mathscr{H}_1$ és $\mathscr{H}_2$ Hilbert-térrel. Mi lesz az összetett rendszerhez tartozó Hilbert-tér? Mik lesznek az összetett rendszer állapotai, illetve mik lesznek a mérések az összetett rendszeren? Ezen kérdések megválaszolásához Hilbert-terek tenzorszorzatára lesz szükségünk.

Függvények tenzorszorzata

1.1.14. Definíció. Az $f_i : \mathscr{X}_i \mapsto \mathbb{K}$ függvények tenzorszorzata, ahol $\mathscr{X}_i$ tetszőleges halmaz $\forall i = 1,...,n$-re, a következő n-változós függvény:

$$f_1 \otimes ... \otimes f_n : (x_1,...,x_n) \mapsto f_1(x_1) \cdot ... \cdot f_n(x_n),\ (x_1,...,x_n) \in \mathscr{X}_1 \times ... \times \mathscr{X}_n$$

1.1.15. Definíció. Egy $v_i \in \mathbb{K}^{d_i}$ vektor egy speciális $v_i : [d_i] \to \mathbb{K}$ függvény, ezért definiálhatjuk vektorok tenzor szorzatát a következőképpen:$v_1 \otimes ... \otimes v_n \in \mathbb{C}^{[d_1]\times...\times[d_n]}$, $(v_1 \otimes ... \otimes v_n)(i_1,...,i_n) = v_1(i_1) \cdot ... \cdot v_n(i_n)$, $(i_1,...i_n) \in [d_1] \times ... \times [d_n]$.

Mátrixokra gondolhatunk úgy, mint függvényekre egy kétszeresen indexelt halmazon, és így ha indexpárok sorozatát $((i_1, j_1),...,(i_n, j_n))$ megfeleltetjük sorozatok indexpárjainak $((i_1,...,i_n),(j_1,...,j_n))$ akkor kapjuk, hogy mátrixok tenzorszorzata a következőképpen hat vektorok tenzorszorzatára:

1.1.16. Definíció. $(A_1 \otimes ... \otimes A_n)(v_1 \otimes ... \otimes v_n) = (A_1v_1) \otimes ... \otimes (A_nv_n)$

Hilbert terek tenzorszorzata

1.1.17. Definíció. Legyenek $\mathscr{H}_1,...,\mathscr{H}_n$ véges dimenziós Hilbert terek. A $\mathscr{H}_1 \otimes ... \otimes \mathscr{H}_n$ tenzorszorzat egy vektortér, amelyet $v_1 \otimes ... \otimes v_n$ alakú vektorok feszítenek ki, ahol $v_i \in \mathscr{H}_i$, úgy hogy $l : (v_1,...,v_n) \mapsto v_1 \otimes ... \otimes v_n$ minden változójában lineáris, azaz $v_1 \otimes ... \otimes v_{i-1} \otimes (v_i + w_i) \otimes .. \otimes v_n = v_1 \otimes ... \otimes v_{i_1} \otimes v_i \otimes v_{i+1} ... \otimes v_n +$

$v_1 \otimes \ldots \otimes v_{i-1} \otimes w_i \otimes v_{i+1} \ldots \otimes v_n$, $v_1 \otimes \ldots \otimes v_{i-1} \otimes (\lambda v_i) \otimes v_{i+1} \ldots \otimes v_n = \lambda v_1 \otimes \ldots \otimes v_{i-1} \otimes v_i \otimes v_{i+1} \ldots \otimes v_n$ minden $i \in [n]$ és $\lambda \in C$

A tenzorszorzat téren megadható egy skalárszorzat, amelyre teljesül a következő tulajdonság:

$\langle x_1 \otimes \ldots \otimes x_n, y_1 \otimes \ldots \otimes y_n \rangle = \langle x_1, y_1 \rangle \cdot \ldots \cdot \langle x_n, y_n \rangle$, $x_i, y_i \in \mathscr{H}_i$

$\mathrm{Tr}(A_1 \otimes \ldots \otimes A_n) = (\mathrm{Tr} A_1) \cdot \ldots \cdot (\mathrm{Tr} A_n)$

1.1.18. Definíció (Parciális nyom)**.** Legyenek $\mathscr{H}_1, .., \mathscr{H}_n$ véges dimenziós Hilbert terek és legyen $\Lambda \subseteq [n]$

A $\bigtimes_{i=1}^{n} Lin(\mathscr{H}_i) \ni (X_1, ..., X_n) \mapsto (\mathrm{Tr}_{\otimes_{i \in \Lambda}} X_i) \otimes_{i \in [n] \setminus \Lambda} X_i = (\prod_{i \in \Lambda} \mathrm{Tr} X_i) \otimes_{i \in [n] \setminus \Lambda} X_i$ egy n-lineáris leképezés, amit parciális nyomnak hívunk $\otimes_{i \in \Lambda} \mathscr{H}_i$ felett és Tr_Λ-val jelöljük.

Pozitív, teljesen pozitív leképezések

1.1.19. Definíció. Legyenek $\mathscr{H}$, $\mathscr{K}$ véges dimenziós Hilbert terek és legyen $\Phi : \mathscr{B}(\mathscr{H}) \mapsto \mathscr{B}(\mathscr{K})$ leképezés. Azt mondjuk, hogy Φ pozitív, ha $\forall A \in \mathscr{B}(\mathscr{H}), A \geq 0$ operátorra $\Phi(A) \geq 0$

1.1.20. Definíció. Legyenek $\mathscr{H}$, $\mathscr{K}$ véges dimenziós Hilbert-terek és legyen $\Phi : \mathscr{B}(\mathscr{H}) \mapsto \mathscr{B}(\mathscr{K})$ lineáris. Azt mondjuk, hogy Φ *n-pozitív*, ha $id_{\mathscr{B}(\mathbb{C}^n)} \otimes \Phi : \mathscr{B}(\mathbb{C}^n) \otimes \mathscr{B}(\mathscr{H}) \mapsto \mathscr{B}(\mathbb{C}^n) \otimes \mathscr{B}(\mathscr{K})$ pozitív.

Φ *teljesen pozitív*, ha $\forall n \in \mathbb{N}$-re n-pozitív.

1.1.21. Definíció. A $\Phi : \mathscr{B}(\mathscr{H}) \mapsto \mathscr{B}(\mathscr{K})$ leképezés *nyomtartó*, ha $\forall A \in \mathscr{B}(\mathscr{H})$ operátorra $\mathrm{Tr}\, \Phi(A) = \mathrm{Tr}\, A$

Megjegyzés. A teljesen pozitív, nyomtartó leképezéseket **kvantumcsatornáknak** is nevezzük.

1.1.22. Tétel (Stinespring reprezentációs tétel)**.** *Legyen Φ teljesen pozitív leképezés. Ekkor $\exists \mathscr{H}_E$ Hilbert-tér és $V : \mathscr{H} \mapsto \mathscr{K} \otimes \mathscr{H}_E$ lineáris leképezés, hogy $\Phi(.) = \mathrm{Tr}_E V(.)V^*$*

A bizonyítás iránt érdeklődő olvasó megtalálhatja azt a [15] cikkben.

Megjegyzés. Ha Φ nyomtartó, akkor V választható izometriának.

2. fejezet

Operátor konvex, operátor monoton függvények

Ebben a fejezetben a [2] könyvre és a [6] cikkre hivatkozunk.

2.0.1. Definíció. Legyen $\mathscr{I} \subseteq \mathbb{R}$ intervallum.

$\mathscr{B}(\mathscr{H})_{sa,\mathscr{I}} = \{A \in B(H)_{sa}, spec(A) \subseteq I\}$

$f : \mathscr{I} \to \mathbb{R}$ **operátor monoton**, ha minden $\mathscr{H}$ véges dimenziós Hilbert-térre, és $\forall A, B \in \mathscr{B}(\mathscr{H})_{sa,\mathscr{I}} A \leq B \Rightarrow f(A) \leq f(B)$

$f : \mathscr{I} \to \mathbb{R}$ **operátor konvex**, ha minden $\mathscr{H}$ véges dimenziós Hilbert-térre és $\forall A, B \in \mathscr{B}(\mathscr{H})_{sa,\mathscr{I}} \forall t \in [0,1] : f((1-t)A + tB) \leq (1-t)f(A) + tf(B)$.

f operátor monoton fogyó, ha $-f$ operátor monoton.

f operátor konkáv, ha $-f$ operátor konvex.

Megjegyzés. A dolgozatban általában az $\mathscr{I} = (0, +\infty)$ esetet vizsgáljuk.

Megjegyzés. f operátor monoton $\Rightarrow f$ monoton

f operátor konvex $\Rightarrow f$ konvex

Ez fordítva nem igaz, pl $t \mapsto t^\alpha$ nem operátor monoton, ha , $\alpha > 1$ és nem operátor konvex, ha $\alpha > 2$.

2.0.2. Példa. *Legyen* $\alpha = 3$ *és legyenek* $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ $\mathbf{B} = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$ *Ekkor* $\mathbf{B} - \mathbf{A} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \geq 0$, *azonban* $\mathbf{B^3} - \mathbf{A^3} = \begin{pmatrix} 30 & 10 \\ 10 & 2 \end{pmatrix}$, *ennek sajátértékei* $\lambda_1 = 16 + 2\sqrt{74}$ *és* $\lambda_2 = 16 - 2\sqrt{74} < 0$, *azaz* $\mathbf{B^3} - \mathbf{A^3}$ *nem pozitív operátor, tehát* $t \mapsto t^3$ *nem operátor monoton.*

2.0.3. Példa. *A lineáris függvények mindig operátor konvexek és konkávok $\mathbb{R}$-en.*

2.0.4. Állítás. *$t \mapsto at+b$ operátor konvex és operátor konkáv $\mathbb{R}$-en és operátor monoton $\iff$ $a \geq 0$ és operátor monoton fogyó $\iff$ $a < 0$.*

Bizonyítás. $f((1-t)A+tB) = a((1-t)A+tB)+b = a(1-t)A+atB+b$

$(1-t)f(A)+tf(B) = a(1-t)A+(1-t)b+taB+tb = a(1-t)A+b-tb+atB+tb = a(1-t)A+atB+b$ Azaz $t \mapsto at+b$ operátor konvex és operátor konkáv $\mathbb{R}$-en.

Legyen $A \leq B$. Ekkor $f(A) = aA+b, f(B) = aB+b$ $f(B)-f(A) = a(B-A)$ Mivel $A \leq B$, ezért $B-A \geq 0$, azaz f operátor monoton $\iff$ $a \geq 0$ és operátor monoton fogyó $\iff$ $a < 0$.

□

2.0.5. Állítás. *$t \mapsto t^2$ operátor konvex $\mathbb{R}$-en.*

Bizonyítás. $(1-t)A^2+tB^2-[(1-t)A+tB]^2 = (1-t)A^2+tB^2-(1-t)^2A^2-t^2B^2-t(1-t)(AB+BA) = t(1-t)[A^2+B^2-AB-BA] = t(1-t)[A-B]^2 \geq 0$ $\forall t \in [0,1]$, $\forall A,B \in \mathscr{B}(\mathscr{H})_{sa}$

□

2.0.6. Lemma. *$t \mapsto \frac{1}{t}$ operátor konvex és operátor monoton fogyó $(0,+\infty)$-n.*

Bizonyítás.

$$(1-t)A^{-1}+tB^{-1}-[(1-t)A+tB]^{-1}$$

$$= B^{-\frac{1}{2}}[(1-t)B^{\frac{1}{2}}A^{-1}B^{\frac{1}{2}}+tI-[(1-t)B^{\frac{-1}{2}}AB^{\frac{-1}{2}}+tI]^{-1}]B^{\frac{-1}{2}}$$

$X := B^{-\frac{1}{2}}AB^{-\frac{1}{2}}$

$x \in (0,+\infty) \to (1-t)x^{-1}+(t-(1-t)x+t)^{-1} \geq 0$ mivel az inverz konvex.$\to X\forall$ sajátértékére teljesül az egyenlőtlenség.

Monotonitás:

Legyenek $A,B \in \mathscr{B}(\mathscr{H})_{sa}, A \leq B \iff B^{-\frac{1}{2}}AB^{-\frac{1}{2}} \leq I \iff \forall\, \lambda \in \mathrm{spec}(B^{-\frac{1}{2}}AB^{-\frac{1}{2}})$:$\lambda \leq 1 \iff \lambda^{-1} \geq 1 \iff \forall \eta \in \mathrm{spec}(B^{\frac{1}{2}}A^{-1}B^{\frac{1}{2}})\ \eta \geq 1 \iff B^{\frac{1}{2}}A^{-1}B^{\frac{1}{2}} \geq I \iff A^{-1} \geq B^{-1}$ □

Következmény: $\forall s > 0\ x \mapsto \frac{x}{x+s} = 1-\frac{s}{x+s} = 1-s\,\mathrm{inv}(x+s)$ operátor konkáv, operátor monoton.

2.0.7. Lemma. *Legyenek $f_1 \ldots f_r$ operátor konvex/konkáv/monoton/monoton fogyó függvények és $c_1 \ldots c_r$ nemnegatív valós számok. Ekkor $c_1 f_1 + \ldots + c_r f_r$ is operátor konvex/konkáv/monoton/monton fogyó, azaz az adott intervallumon operátor konvex/konkáv/monoton/monoton fogyó függvények konvex kúpot alkotnak.*

2.1. Operátor konvex, operátor monoton függvények integrálreprezentációja

2.1.1. Állítás. *Legyen μ véges mérték a pozitív félegyenes Borel-halmazain, $a \in \mathbb{R}, b \in \mathbb{R}_+$. Ekkor*

$$f(x) := a + bx + \int_0^{+\infty} \frac{x}{x+s}(1+s)d\mu(s) \; x \in [0, +\infty)$$

operátor monoton $[0, +\infty)$-en.

Megjegyzés. Minden operátor monoton függvény $[0, +\infty)$-en így áll elő.

Legyen μ véges mérték a $(0, +\infty)$ Borel-halmazain, legyenek $a, b \in \mathbb{R}, c \in \mathbb{R}_+$.

$$f(x) := a + bx + cx^2 + \int_0^{+\infty} \left(\frac{x}{1+s} + \frac{x}{x+s}\right)(1+s)^2 d\mu(s)$$

operátor konvex.

Megjegyzés. Minden operátor konvex függvény így áll elő $(0, +\infty)$-n. A bizonyítást lásd [2] könyv V. fejezetében vagy a [7] cikk V. szekciójában.

Megjegyzés. Legyen f operátor monoton $[0, +\infty)$-n. Ekkor

$$\lim_{x \to \infty} \frac{f(x)}{x} = b + \lim_{x \to \infty} \int_0^{+\infty} \frac{1}{x+s}(1+s)d\mu(s) = b$$

$\to$ egy operátor monoton függvény nem nőhet lineárisnál gyorsabban $\to t \mapsto t^\alpha$ nem operátor monoton növő ha $\alpha > 1$. A bizonyításhoz lásd a [2] könyv IV. fejezetét.

Hasonlóan, legyen f operátor konvex $(0, +\infty)$-n. Ekkor $\lim\limits_{x \to \infty} \frac{f(x)}{x^2} = c \to$ az operátor konvex függvények nem nőhetnek kvadratikusnál gyorsabban.Speciálisan, $t \mapsto t^\alpha$ nem operátor konvex ha $\alpha > 2$

2.1.2. Példa.

$$\int_0^{+\infty} \frac{1}{1+s} - \frac{1}{x+s} ds = \lim_{y \to \infty} [\log \frac{1+s}{x+s}]_0^y = \log x$$

x-ben operátor monoton növő, operátor konkáv $\to$ log *operátor monoton növő és operátor konkáv.*

2.1.3. Példa.

$$x\log x = \int\limits_0^{+\infty} \frac{x}{1+s} - \frac{x}{x+s} ds = \int\limits_0^{+\infty} (\frac{x}{1+s} - \frac{x}{x+s})(1+s)^2 \frac{1}{(1+s)^2} ds$$

$$= \int\limits_0^{+\infty} (\frac{x}{1+s} - \frac{x}{x+s})(1+s)^2 d\mu(s)$$

$\to x \mapsto x\log x$ *operátor konvex.*

Megjegyzés. Operátor konvex függvényekre is igaz a Jensen-egyenlőtlenség, azaz ha $A_1 \ldots A_r \in \mathscr{B}(\mathscr{H})_{sa,\mathscr{I}}$ $t_1, \ldots t_r t_i \geq 0$ $\forall i$ úgy, hogy $\sum t_i = 1$ akkor

$$f(\sum_{i=1}^{r} t_i A_i) \leq \sum_{i=1}^{r} t_i f(A_i),$$

ha f operátor konvex.

2.2. $\mathrm{Tr}\circ f$ tulajdonságai

Láttuk:

f monoton $\not\Rightarrow$ f operátor monoton

f konvex $\not\Rightarrow$ f operátor konvex

Azonban

f monoton $\implies$ $\mathrm{Tr}\circ f$ monoton.

f konvex $\implies$ $\mathrm{Tr}\circ f$ konvex.

2.2.1. Lemma (Courant–Fischer–Weyl minimax tétel)**.** *Legyen $A \in \mathscr{B}(\mathscr{H})_{sa}$. Legyenek $\lambda_1^{\downarrow}(A),\dots,\lambda_d^{\downarrow}(A)$ A csökkenő sorrendben rendezett sajátértékei. Ekkor:*

$$\lambda_k^{\downarrow}(A) = \max_{\mathscr{K}\subseteq\mathscr{H}} \min\{\langle x, Ax\rangle : x \in \mathscr{K}\, ||x|| = 1, \dim\mathscr{K} = k\}$$

Bizonyítás. Legyen $e_1,\dots,e_d$ ortonormált bázis. $Ae_i = \lambda_i^{\downarrow}(A)e_i$ $\mathscr{H}_{[1,k]} := \{e_1,\dots,e_k\}$, $x = \sum_{i=1}^{k} \langle e_i, x\rangle e_i$, $\langle x, Ax\rangle = \sum_{i=1}^{k} |\langle e_i, x|^2 \lambda_i^{\downarrow}(A) \geq \lambda_k^{\downarrow}(A)$

$\mathscr{H}_{[k,d]} := \mathrm{span}\{e_k,\dots,e_d\}$

$\dim\mathscr{H}_{[k,d]} = d-k+1 \implies \dim\mathscr{K} = k \implies \mathscr{K}\cap\mathscr{H}_{[k,d]} \neq \{0\}$ Legyen $x \in \mathscr{K}\cap\mathscr{H}_{[k,d]}, ||x|| = 1$

$$\langle x, Ax\rangle = \sum_{i=k}^{d} |\langle e_i, x\rangle|^2 \lambda_i^{\downarrow}(A) \leq \lambda_k^{\downarrow}(A) \qquad \square$$

Következmény:

$A, B \in \mathscr{B}(\mathscr{H})_{sa,I}, A \leq B \implies \forall k$-ra $\lambda_k^{\downarrow}(A) \leq \lambda_k^{\downarrow}(B)$

2.2.2. Állítás. *Legyen $\mathscr{I} \subseteq \mathbb{R}$ intervallum, $f : \mathscr{I} \mapsto \mathbb{R}$ monoton.*

Ekkor $\mathrm{Tr}\circ f$ *monoton $\mathscr{B}(\mathscr{H})_{sa,\mathscr{I}}$-n.*

Bizonyítás. $A, B \in \mathscr{B}(\mathscr{H})_{sa,\mathscr{I}}, A \leq B$

$$\mathrm{Tr} f(A) = \sum_{k=1}^{d} f(\lambda_k^{\downarrow}(A)) \leq \sum_{k=1}^{d} f(\lambda_k^{\downarrow}(B)) = \mathrm{Tr} f(B) \qquad \square$$

f konvex $\implies$ $\mathrm{Tr}\circ f$ konvex.

Bizonyítás: erősebb formában.

2.2.3. TÉTEL. *$f : \mathscr{I} \mapsto \mathbb{R}$ konvex $\Longrightarrow$ $\mathrm{Tr} \circ f$ operátor együtthatókkal konvex, azaz*

$\forall A_i \in \mathscr{B}(\mathscr{H}_i)_{sa,\mathscr{I}}$ $\forall K_i \in \mathscr{B}(\mathscr{K},\mathscr{H}_i)$: $\sum\limits_{i=1}^{r} K_i^* K_i = I_{\mathscr{K}}$:

$\mathrm{Tr}\, f(\sum\limits_{i=1}^{r} K_i^* A_i K_i) \leq \mathrm{Tr} \sum\limits_{i=1}^{r} K_i^* f(A_i) K_i$

$\overline{A} := \sum\limits_{i=1}^{r} K_i^* A_i K_i$

Bizonyítás. $\overline{A} = \sum\limits_{k=1}^{d} \lambda_k |e_k\rangle e_k|$

f konvex $\Longrightarrow$ $\forall k$ $\exists e_k(t) = c_k(t) + b_k : f(t) \geq e_k(t)$ $\forall t \in \mathscr{I}$ és egyenlőség λ_k-ban van.

$\mathrm{Tr}\, f(\overline{A}) = \sum\limits_{k=1}^{r} f(\lambda_k) = \sum\limits_{k=1}^{r} e_k(\lambda_k) = \sum\limits_{k=1}^{r} \langle e_k, (c_k(\overline{A}) + b_k I) e_k\rangle = \sum\limits_{k=1}^{r} \langle e_k, (c_k \sum\limits_{i=1}^{r} K_i^* A_i K_i + b_k I) e_k\rangle \leq \sum\limits_{k=1}^{r} \langle e_k, \sum\limits_{i=1}^{r} K_i^* f(A_i) K_i e_k\rangle = \mathrm{Tr} \sum\limits_{i=1}^{r} K_i^* f(A_i) K_i$ □

2.3. Blokkdiagonalizálás

2.3.1. Állítás. *Legyenek $P_i, ..., P_r \in \mathscr{B}(\mathscr{H})$ projekciók. A következők ekvivalensek:*

i, $P_1 + ..., P_r = I$

ii, $\mathrm{ran}\, P_i \perp_{i \neq j} \mathrm{ran}\, P_j$ *és* $\mathrm{span}\{\mathrm{ran}\, P_i : i \in [r]\} = \mathscr{H}$

Bizonyítás. Tegyük fel, hogy $P_1 + ..., P_r = I$. Ekkor bármely $\psi \in \mathscr{H}$-ra $\psi = I\psi = P_1\psi + ..., P_r\psi$ és így $\psi \in \mathrm{span}\{\mathrm{ran}\, P_i : i \in [r]\} = \mathscr{H}$, azaz $\mathrm{span}\{\mathrm{ran}\, P_i : i \in [r]\} = \mathscr{H}$. Tegyük fel, hogy léteznek $i \neq j$ úgy, hogy $\mathrm{ran}\, P_i \not\perp \mathrm{ran}\, P_j$. Ez azt jelenti,hogy létezik $\psi \neq 0$ vektor, $\psi \in \mathrm{ran}\, P_j$ úgy, hogy $P_j\psi \neq 0$. Ezért $||\psi||^2 = \langle\psi, I\psi\rangle \geq \langle\psi, P_i\psi\rangle + \langle\psi, P_j\psi\rangle = ||\psi||^2 + \langle\psi, P_j\psi\rangle > ||\psi||^2$, ami ellentmondás. Tegyük fel most, hogy $\mathrm{ran}\, P_i \perp_{i \neq j} \mathrm{ran}\, P_j$ és $\mathrm{span}\{\mathrm{ran}\, P_i : i \in [r]\} = \mathscr{H}$. Az utóbbiból adódik, hogy bármely $\psi \in \mathscr{H}$-ra léteznek $\psi \in \mathrm{ran}\, P_i$, hogy $\psi = \psi_1 +, ..., \psi_r$. Az ortogonalitási feltétel miatt $P_i\psi = \psi_i$, amiből $I\psi = \psi = P_1\psi + ... + P_r\psi = (P_1 + ... + P_r)\psi$ és így $P_1 + ..., P_r = I$ □

Megjegyzés. A fenti $P_1 + ..., P_r = I$ felbontást **egységosztásnak** hívjuk.

2.3.2. Definíció. Legyen $P_1 + ..., P_r = I$ egységosztás, $X \in \mathscr{B}(\mathscr{H})$ operátor. Ekkor az X $\{P_i\}_{i=1}^r$ egységosztás szerinti **blokkdiagonalizáltja**:$\mathscr{P}_{\{Pi\}}X := \sum_{i=1}^{r} P_i X P_i$.

Ha $\sigma \in \mathscr{B}(\mathscr{H})_{sa}, \sigma = \sum_{i=1}^{r} s_i P_i$, akkor $\mathscr{P}_\sigma X := \mathscr{P}_{\{P_i\}}X$

2.4. A Fréchet-derivált

2.4.1. Definíció. Legyen $I \subseteq \mathbb{R}$ nyílt intervallum, f differenciálható I-n. Ekkor az $f^{[1]}$ függvényt a következőképpen definiáljuk $I \times I$-n:

$$f^{[1]}(\lambda, \mu) = \begin{cases} \frac{f(\lambda)-f(\mu)}{\lambda-\mu} & \text{ha } \lambda \neq \mu \\ f'(\lambda) & \text{ha } \lambda = \mu \end{cases}$$

$f^{[1]}(\lambda, \mu)$-t az f **első különbségihányados függvényének** nevezzük a (λ, μ) helyen.

2.4.2. Definíció. Az f függvény **(Fréchet-értelemben) differenciálható** A-ban ($A \in \mathscr{B}(\mathscr{H})$), ha létezik $f'(A)$ lineáris leképezés, hogy minden $H \in \mathscr{B}(\mathscr{H})$-ra:

$$\lim_{||H|| \to 0} \frac{||f(A+H) - f(A) - f'(A)(H)||}{||H||} = 0$$

2.4.3. Állítás. *$f'(A) : X \mapsto \sum_{i,j=1}^{d} f^{[1]}(a_i, a_j) P_i X P_j$, ahol $A = \sum_{i=1}^{d} a_i P_i$*

Az állítás bizonyítása megtalálható a [2] könyv V. fejezetében.

2.4.4. Állítás. *Jelölje $spec(X)$ egy operátor nemnulla sajátértékeinek halmazát. Ekkor $spec(AB) = spec(BA)$.*

Bizonyítás. Ha $\lambda \in spec(AB)$, akkor $\exists v \in \mathscr{H}$ vektor, amelyre $ABv = \lambda v$

Kell, hogy létezik w, amelyre $BAw = \lambda w$. Legyen $w = Bv$, ekkor $BAw = BABv = B(ABv) = B(\lambda v) = \lambda Bv = \lambda w$, azaz kaptuk, hogy $spec(AB) \subseteq spec(BA)$.

Kell még, hogy ha $\lambda \in spec(BA)$, akkor $\lambda \in spec(AB)$. Létezik $w \in \mathscr{H}$, amelyre $BAw = \lambda w$. Legyen $v = Aw$, ekkor $ABv = ABAw = A(BAw) = A\lambda w = \lambda Aw = \lambda v$, azaz $spec(BA) \subseteq spec(AB)$ $\square$

2.4.5. Állítás. *Legyen $F : A \mapsto \operatorname{Tr} f(A)$. Ekkor*

$$F'(A)(X) = \operatorname{Tr} f'(A)X$$

Bizonyítás.

$$\operatorname{Tr} f'(A)(X) = \operatorname{Tr} \sum_{i,j=1}^{d} f^{[1]}(a_i,a_j) P_i X P_j = \sum_{i,j=1}^{d} \operatorname{Tr} f^{[1]}(a_i,a_j) P_i X P_j$$

$$= \sum_{i,j=1}^{d} f^{[1]}(a_i,a_j) \operatorname{Tr} P_i X P_j = \sum_{i,j=1}^{d} f^{[i]}(a_i,a_j) \operatorname{Tr} P_j P_i X$$

P_i, P_j ortogonális projekciók, ezért:

$$= \sum_{i=1}^{d} f^{[1]}(a_i,a_i) \operatorname{Tr} P_i X = \sum_{i=1}^{d} f'(a_i) \operatorname{Tr} P_i X = \operatorname{Tr} f'(A) X.$$

$\square$

3. fejezet

Rényi-divergenciák

3.1. Motiváció

Tekintsük a következő problémát: Alice egy bitnyi információt szeretne küldeni Bobnak. Ezt úgy teszi, hogy a 0-t belekódolja egy $\rho \in S(\mathscr{H})$, az 1-et pedig egy $\sigma \in S(\mathscr{H})$ kvantumállapotba, majd azt átküldi Bobnak, aki a $(T(0), T(1)) \in POVM\{0,1\}, \mathscr{H}$ dekódolja, amelynek a lehetséges kimenetelei (0,1) ahol $T(0)$, $T(1) \geq 0$, $T(0) + T(1) = I$. Ha a mérés eredményeként 0-t kap, akkor arra következtet, hogy Alice 0-t küldött, ha pedig 1-et mér, akkor arra következtet, hogy Alice 1-et küldött. Kétféle hiba léphet fel a folyamat során: Alice 0-t küld, de Bob 1-et dekódol (elsőfajú hiba), illetve fordítva, Alice 1-et küld, de Bob 0-t dekódol (másodfajú hiba). Jelölje $\alpha(T)$ az elsőfajú hiba, $\beta(T)$ a másodfajú hiba valószínűségét. A Born-szabályból kapjuk, hogy $\alpha(T) = \operatorname{Tr} \rho T(1) = \operatorname{Tr} \rho (I - T(0))$, $\beta(T) = \operatorname{Tr} \sigma T(0)$.

A fenti feladat számos érdekes kérdést vet fel: mik a tökéletesen megkülönböztethető állapotok? Hogyan csökken a hibavalószínűség, ha többször küldjük el az üzenetet? Ezen kérdések megválaszolása különféle információelméleti mennyiségek definiálását motiválja. Ebben a fejezetben a fő célunk a [10] és a [17] cikkekben bevezetett úgynevezett szendvicselt Rényi-divergenciák fogalmának és matematikai tulajdonságainak bemutatása az [5] cikket követve. Ehhez előbb áttekintjük a klasszikus f-divergenciák fogalmát a [4] cikk alapján, illetve a sztenderd kvantum Rényi-divergenciákat a [13] cikk alapján.

3.2. f-divergenciák

Az f-divergenciák fogalmát Csiszár Imre magyar matematikus vezette be a klasszikus esetre, majd Petz Dénes magyar matematikus általánosította a kvantum esetre. Szerepük az információelméletben kiemelkedő, sok különböző fogalom tárgyalható f-divergenciák speciális eseteként. Az alábbi alfejezetben bevezetjük a klasszikus f-divergenciákat, megvizsgáljuk néhány fontos tulajdonságukat, majd a Rényi-divergenciáknál és a relatív entrópiánál megmutatjuk, hogy hogyan származtathatók ezek az f-divergenciákból.

Legyen $f:(0,+\infty)\mapsto\mathbb{R}$ olyan, hogy $\exists f(0^+):=\lim_{t\searrow 0} f(t)$ és $\exists\ \omega(f):=\lim_{t\to+\infty}\frac{f(t)}{t}$, és ezek nem ellenkező előjelű végtelenek.

3.2.1. Definíció. $\mathscr{P}_f(t,s):=sf(\frac{t}{s})$, $t,s\in(0,+\infty)$ az f-hez tartozó **perspektíva-függvény**.

Megjegyzés. $\mathscr{P}_f(t,1)=f(t)\ \forall t$

$\hat{f}(s)=\mathscr{P}_f(1,s)=sf(\frac{1}{s})$ a **transzponált függvény**

$\mathscr{P}_{\hat{f}}(t,s)=\mathscr{P}_f(s,t)$

Kiterjesztés a $[0,+\infty)^2$-re.

$$\lim_{\varepsilon\searrow 0}\mathscr{P}_f(t+\varepsilon,s+\varepsilon)=\begin{cases} sf(\frac{t}{s}) & t,s>0\\ sf(0^+) & t=0\\ t\omega(f) & s=0\end{cases}$$

Észrevétel: $\mathscr{P}_f$ homogén.

$\forall c>0\ \mathscr{P}_f(ct,cs)=csf(\frac{ct}{cs})=c\mathscr{P}_f(t,s)$

3.2.2. Lemma (Általánosított log-összeg egyenlőtlenség)**.** *Legyen $f:(0,+\infty)\mapsto\mathbb{R}$ konvex.*

$a_i,b_i\in(0,+\infty)$, $i=1,\dots,r$

$a:=\sum_{i=1}^r a_i$, $b_i:=\sum_{i=1}^r b_i\implies bf\left(\frac{a}{b}\right)\leq\sum_{i=1}^r b_if\left(\frac{a_i}{b_i}\right)$

Bizonyítás. A Jensen-egyenlőtlenség szerint:$f\left(\sum_{i=1}^r\frac{b_i}{b_i}\cdot\frac{a_i}{b_i}\right)\leq\sum_{i=1}^r\frac{b_i}{b_i}f\left(\frac{a_i}{b_i}\right)$ ☐

Következmény: f konvex $\Longrightarrow \mathscr{P}_f$ szubadditív, azaz $\mathscr{P}_f\left(\sum_{i=1}^r a_i, \sum_{i=1}^r b_i\right) \leq \sum_{i=1}^r \mathscr{P}_f(a_i,b_i)$
$\Longrightarrow \mathscr{P}_f$ konvex, mert $\mathscr{P}_f\left(\sum_{i=1}^r p_i t_i, \sum_{i=1}^r p_i s_i\right) \leq \sum_{i=1}^r \mathscr{P}_f(p_i t_i, p_i s_i) \leq \sum_{i=1}^r p_i \mathscr{P}_f(t_i,s_i)$

Következmény: $f\colon (0,+\infty) \mapsto \mathbb{R}$ ekvivalensek a következők:

1, f konvex

2, $\hat{f}$ konvex

3, $\mathscr{P}_f$ konvex

3.2.3. Definíció. $f:(0,+\infty)\mapsto \mathbb{R}^+$, $\exists f(0^+), \omega(f)$, nem ellenkező előjelű végtelenek. $p,q \in \mathbb{R}_+^{\mathscr{X}}$. Ekkor p-nek a q-ra vett f függvényhez tartozó f-divergenciája:

$$D_f(p||q) := \sum_{x\in\mathscr{X}} \mathscr{P}_f(p(x),q(x)) =$$

$$\sum_{x:q(x),p(x)>0} q(x) f(\frac{p(x)}{q(x)}) + \sum_{x:p(x)=0} q(x)f(0^+) + \sum_{x:q(x)=0} p(x)\omega(f) =$$

$$\sum_{x:p(x),q(x)>0} q(x) f(\frac{p(x)}{q(x)} + f(0^+)q(\{p=0\}) + \omega(f)p(\{q=0\}).$$

Példa:

$f(t) := \eta(t) = t\log t$

$$D_\eta(p||q) = \sum_{x:p(x),q(x)>0} q(x)\frac{p(x)}{q(x)}\log\frac{p(x)}{q(x)} + (+\infty)p(q=0)$$

$$D_\eta(p||q) = \begin{cases} \sum_x p(x)(\log p(x) - \log q(x)) & \text{ha } p \ll q \\ +\infty & \text{egyébként} \end{cases}$$

$f_\alpha(t) = t^\alpha \ \alpha > 0, \alpha \neq 1$

$$D_{f_\alpha}(p||q) = \begin{cases} \sum_x p(x)^\alpha q(x)^{1-\alpha} & \alpha \in (0,1) \text{ vagy } p \ll q \\ +\infty & \text{különben} \end{cases}$$

3.3. Entropikus mennyiségek

3.3.1. Definíció. Legyenek $\rho,\sigma \in S(\mathscr{H})$ állapotok. Ekkor ρ,σ **relatív entrópiája**

$$D(\rho||\sigma) = \begin{cases} \operatorname{Tr}\rho(\log^*\rho - \log^*\sigma) & \text{ha } \rho^0 \leq \sigma^0 \text{ vagy } \alpha \in (0,1) \\ +\infty & \text{különben} \end{cases}$$

Ahol $\log^*(t) := \log(t), t > 0$ és $\log^*(t) := 0$, $t = 0$ ρ^0, σ^0 a ρ illetve σ tartójára vetítő projekciót jelöli.

3.3.2. Definíció. Legyenek $\rho, \sigma \in S(\mathscr{H})$ állapotok, és $\alpha \in \mathbb{R}$. Ekkor

$$\Psi(\alpha) := \log \operatorname{Tr} \rho^\alpha \sigma^{1-\alpha},$$

ahol azt a konvenciót használjuk, hogy egy pozitív szemidefinit operátor hatványai csak a tartóján vannak definiálva, azaz ha $\sigma = \sum\limits_{s \in spec(\sigma)} sP^\sigma(s)$, akkor $\sigma^\beta = \sum\limits_{s \in spec(\sigma), s>0} s^\beta P^\sigma(s)$

3.3.3. Definíció. Legyenek $\rho, \sigma \in S(\mathscr{H})$ állapotok, és $\alpha \in [0, +\infty) \setminus \{1\}$. Ekkor ρ, σ **Rényi-divergenciája** vagy **α-relatív entrópiája** a következő:

$$D_\alpha(\rho||\sigma) = \begin{cases} \frac{1}{\alpha-1} \log \operatorname{Tr} \rho^\alpha \sigma^{1-\alpha} & \text{ha } \rho^0 \leq \sigma^0 \text{ vagy } \alpha \in [0,1) \\ +\infty & \text{különben} \end{cases}$$

3.3.4. Állítás. *Ha $\rho^0 \leq \sigma^0$ akkor $\Psi'(1) = D(\rho||\sigma)$, ha pedig $\rho^0 \geq \sigma^0$, akkor $\Psi'(0) = -D(\rho||\sigma)$*

Bizonyítás. Legyenek $\lambda_1, ..., \lambda_n$ ρ nemnegatív sajátértékei, $P_1, ..., P_n$ pedig a hozzájuk tartozó spektrális projekciók, legyenek továbbá $\eta_1, ..., \eta_m$ σ nemnulla sajátértékei, a hozzájuk tartozó spektrális projekciók pedig $Q_1, ..., Q_m$.

Ekkor $\operatorname{Tr} \rho^\alpha \sigma^{1-\alpha} = \operatorname{Tr}(\sum\limits_{i=1}^n \lambda_i P_i)(\sum\limits_{j=1}^m \eta_j^{1-\alpha} Q_j) = \sum\limits_{i=1}^n \sum\limits_{j=1}^m \lambda_i^\alpha \eta_j^{1-\alpha} \operatorname{Tr} P_i Q_j$

Ahonnan $\Psi'(\alpha) = \frac{1}{\operatorname{Tr} \rho^\alpha \sigma^{1-\alpha}} \sum\limits_{i=1}^n \sum\limits_{j=1}^m \lambda_1^\alpha \eta_j^{1-\alpha} (\log \lambda_i - \log \eta_j) \operatorname{Tr} P_i Q_j =$

$= \frac{1}{\operatorname{Tr} \rho^\alpha \sigma^{1-\alpha}} \operatorname{Tr} \rho^\alpha \sigma^{1-\alpha} (\log^* \rho - \log^* \sigma)$ amiből $\Psi'(1) = \frac{1}{\operatorname{Tr} \rho \sigma^0} \operatorname{Tr} \rho \sigma^0 (\log^* \rho - \log^* \sigma)$
Ha $\rho^0 \leq \sigma^0$, akkor $\rho \sigma^0 = \rho$ és a fenti formula éppen $D(\rho||\sigma)$

Hasonlóan, $\Psi'(0) = \frac{1}{\operatorname{Tr} \rho^0 \sigma} \operatorname{Tr} \rho^0 \sigma (\log^* \rho - \log^* \sigma)$. Ha $\rho^0 \geq \sigma^0$, akkor $\rho^0 \sigma = \sigma$, amiből a fenti egyenlőség $-D(\rho||\sigma)$-vá redukálódik. □

3.3.5. Definíció. Legyen $\mathscr{X}$ véges halmaz, és P valószínűségeloszlás $\mathscr{X}$-en, f pedig $\mathscr{X} \mapsto \mathbb{R}$ függvény. Ekkor f P-re vonatkozó várható értéke:$E_P(f) = \sum\limits_{x \in \mathscr{X}} P(x) f(x)$.
f P-re vonatkozó varianciája pedig $V_P(f) = E_P(f^2) - E_P(f)^2$

3.3.6. Állítás. *Ψ konvex $\mathbb{R}$-en és vagy affin függvény, vagy $\Psi''(\alpha) > 0$ minden $\alpha \in \mathbb{R}$ esetén.*

Bizonyítás. Az előző állítás bizonyításában látottakat folytatva

$$\Psi\text{"}(\alpha) = \frac{1}{\operatorname{Tr}\rho^\alpha\sigma^{1-\alpha}}\sum_{i=1}^{n}\sum_{j=1}^{m}\lambda_i^\alpha\eta_j^{1-\alpha}(\log\lambda_i - \log\eta_j)^2\operatorname{Tr}P_iQ_j -$$
$$\left(\frac{1}{\operatorname{Tr}\rho^\alpha\sigma^{1-\alpha}}\right)^2\left(\sum_{i=1}^{n}\sum_{j=1}^{m}\lambda_i^\alpha\eta^{1-\alpha}(\log\lambda_i - \log\eta_j)\operatorname{Tr}P_iQ_j\right)^2 =$$
$$\sum_{i=1}^{n}\sum_{j=1}^{m} f(i,j)^2 p_\alpha(i,j) - \left(\sum_{i=1}^{n}\sum_{j=1}^{m} f(i,j)p_\alpha(i,j)\right)^2,$$

ahol $f(i,j) := \log\lambda_i - \log\eta_j$, és $p_\alpha(i,j) := \frac{\lambda_i^\alpha\eta_j^{1-\alpha}}{\operatorname{Tr}\rho^\alpha\sigma^{1-\alpha}}$, ami valószínűségeloszlást definiál $[n]\times[m]$-n. Ekkor a fenti formula nem más, mint f p_α-ra vonatkozó varianciája, és mivel ez nemnegatív, adódik, hogy Ψ konvex.Ψ második deriváltja pontosan akkor 0, ha f p_α-ra vonatkozó varianciája 0, ami ekvivalens azzal, hogy f konstans p_α tartóján. Azonban p_α tartója $[n]\times[m]$, ami független α-tól.Így $\Psi\text{"}(\alpha) = 0$ minden $\alpha\in\mathbb{R}$, amiből Ψ affin, vagy pedig $\Psi\text{"}(\alpha) > 0$ minden $\alpha\in\mathbb{R}$-re. □

3.3.7. Állítás. *$D_1(\rho||\sigma) := \lim_{\alpha\to 1} D_\alpha(\rho||\sigma) = D(\rho||\sigma)$, és $\alpha\mapsto D_\alpha(\rho||\sigma)$ monoton növő $(0,+\infty)$-n.*

Bizonyítás. Tegyük fel, hogy $\rho^0 \le \sigma^0$. Ekkor $\Psi(1) = \log\operatorname{Tr}\rho\sigma^0 = \log\operatorname{Tr}\rho = 0$, és így $D_\alpha(\rho||\sigma) = \frac{\Psi(\alpha)-\Psi(1)}{\alpha-1}$, amiben az $\alpha\to 1$ határátmenetet véve definíció szerint $\Psi'(1)$-t kapjuk, ami a korábban látottak alapján $D(\rho||\sigma)$.

Tegyük fel most, hogy $\rho^0 \not\le \sigma^0$. Ekkor $D_\alpha(\rho||\sigma) = +\infty = D(\rho||\sigma)$ minden $\alpha >$ 1-re, és így $\lim_{\alpha\searrow 1} = D(\rho||\sigma)$ Ekkor $\Psi(1) = \log\operatorname{Tr}\rho\sigma^0 < 0$, és így $D_\alpha(\rho||\sigma) = \frac{\Psi(\alpha)-\Psi(1)}{\alpha-1} + \frac{\Psi(1)}{\alpha-1}$. Az előbbi formula első tagja Ψ 1-beli deriváltjához tart, ha $\alpha\nearrow 1$, míg a második tag $+\infty$-hez tart, ami ez esetben $D(\rho||\sigma)$.

Végül, mivel Ψ konvex, ezért $\alpha\mapsto\frac{\Psi(\alpha)-\Psi(1)}{\alpha-1}$ monoton növő, és mivel $\Psi(1)\le 0$, így $\alpha\mapsto\frac{\Psi(1)}{\alpha-1}$ is monoton növő, amiből a fenti felbontásból adódik, hogy $\alpha\mapsto D_\alpha(\rho||\sigma)$ monoton növő. □

3.3.8. Állítás. *Minden $\alpha\in(0,1)$ és minden $\rho,\sigma\in\mathscr{S}(\mathscr{H})$ D_α pozitív, azaz $D_\alpha(\rho||\sigma)\ge 0$ és egyenlőség pontosan akkor áll fenn, ha $\rho = \sigma$*

Bizonyítás. $D_\alpha(\rho||\sigma) = \frac{1}{\alpha-1}\log\operatorname{Tr}\rho^\alpha\sigma^{1-\alpha}$

Legyenek $p := \frac{1}{\alpha}, q := \frac{1}{1-\alpha}$. Ekkor $\frac{1}{p}+\frac{1}{q} = 1$. A Hölder-egyenlőtlenség szerint:

$$|\operatorname{Tr}\rho^\alpha\sigma^{1-\alpha} \le ||\rho^\alpha||_{\frac{1}{\alpha}}||\sigma^{1-\alpha}||_{\frac{1}{1-\alpha}}$$

$$= (\operatorname{Tr}\rho^{\frac{\alpha}{\alpha}})^{\alpha}(\operatorname{Tr}\sigma^{\frac{1-\alpha}{\alpha}})^{1-\alpha} = 1.$$

Azaz $\operatorname{Tr}\rho^{\alpha}\sigma^{1-\alpha} \leq 1 \implies \log\operatorname{Tr}\rho^{\alpha}\sigma^{1-\alpha} \leq 0$. Mivel $\alpha - 1 < 0$, így

$$\frac{1}{\alpha-1}\log\operatorname{Tr}\rho^{\alpha}\sigma^{1-\alpha} \geq 0.$$

Egyenlőség akkor állhat fenn, ha $\rho = c\sigma$, azonban ρ, σ állapotok, így c csak 1 lehet. □

3.3.1. Szendvicselt Rényi-divergenciák

A következőkben egy újfajta Rényi-divergenciát definiálunk, összehasonlítjuk a korábban definiálttal, illetve belátjuk néhány fontos tulajdonságát. Az alábbiakban definiált mennyiség szoros kapcsolatban áll más kvantum-információelméleti fogalmakkal, megjelenik a fejezet elején bemutatott állapotmegkülönböztetési problémában, mint egy "trade-off" az első-és másodfajú hibavalószínűségek jellemzésében, illetve fontos szerephez jut a kvantum statisztikus fizikában.

3.3.9. Definíció. Legyen $A \in \mathscr{B}(\mathscr{H})$. Ekkor A Schatten-féle p-normája a következő:

$||A||_p = (\operatorname{Tr}|A|^p)^{\frac{1}{p}}$, $p > 1$

Megjegyzés. $p \to +\infty$ esetén az operátornormát kapjuk.

3.3.10. Definíció. [10]

$$D^*_{\alpha}(\rho||\sigma) = \begin{cases} \frac{1}{\alpha-1}\log(\operatorname{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^{\alpha} & \text{ha } \alpha \in (0,1)\cup(1,+\infty) \\ \operatorname{Tr}\rho(\log\rho - \log\sigma) & \text{ha } \alpha = 1 \\ \log||\sigma^{\frac{-1}{2}}\rho\sigma^{\frac{-1}{2}}||_{\infty} & \text{ha } \alpha = \infty \end{cases}$$

ahol $\operatorname{Tr}(\sigma^{\frac{1-\alpha}{\alpha}}\rho\sigma^{\frac{1-\alpha}{\alpha}})^{\alpha}$-t végtelennek definiáljuk, ha $\rho^0 \not\leq \sigma^0$.

A klasszikus és szendvicselt Rényi-divergenciák összehasonlításában a következő egyenlőtlenség lesz segítségünkre:

3.3.11. Állítás (Lieb-Thirring egyenlőtlenség)**.** *Legyenek $A, B \geq 0$ operátorok és $r \geq 1$. Ekkor* $\operatorname{Tr}(BAB)^r \leq \operatorname{Tr}(B^rA^rB^r)$

Az érdeklődő olvasó megtalálhatja a bizonyítást a [8] cikkben.

3.3.12. Állítás. *Ha $\alpha > 1$, akkor a klasszikus Rényi-divergencia felülről becsli a szendvicseltet, azaz $D^*_{\alpha}(\rho||\sigma) \leq D_{\alpha}(\rho||\sigma)$*

Bizonyítás. Alkalmazzuk a Lieb-Thirring egyenlőtlenséget a következő választással: $B := \sigma^{\frac{1-\alpha}{2\alpha}}, A := \rho, r := \alpha$, amiből adódik, hogy $\mathrm{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^{\alpha} \leq \mathrm{Tr}(\sigma^{\frac{1-\alpha}{2}} \rho^{\alpha} \sigma^{\frac{1-\alpha}{2}})$, ahonnan felhasználva a nyom ciklikusságát:$\mathrm{Tr}(\sigma^{\frac{1-\alpha}{2}} \rho^{\alpha} \sigma^{\frac{1-\alpha}{2}}) = \mathrm{Tr}(\rho^{\alpha} \sigma^{1-\alpha})$ □

A következőkben a szendvicselt Rényi-divergenciák további fontos tulajdonságait vizsgáljuk. Ehhez szükségünk lesz az úgynevezett diszkrét Weyl-operátorokra.

3.4. Diszkrét Weyl-operátorok

3.4.1. Definíció. Legyen $f_0, ..., f_{d-1}$ ortonormált bázis egy d-dimenziós Hilberttérben. Definiáljuk az X, Z operátorokat a következőképpen: $X f_k := f_{k+1}$, $Z f_k := e^{i \frac{2\pi}{d} k} f_k$, $k \in \{0, ..., d-1\}$, ahol az összeadás *mod d* értendő.

Megjegyzés. X, Z a kvantumbitek x és z Pauli-operátorainak d-dimenziós rendszerre vett általánosításai

Legyenek a **diszkrét Weyl-operátorok** a következők:

$W_{a,b} := X^a Z^b \; a, b \in \{0, ..., d-1\}$

3.4.2. Állítás. $ZX = e^{i \frac{2\pi}{d}} XZ$

Bizonyítás. $ZX f_k = Z f_{k+1} = e^{i \frac{2\pi}{d}(k+1)} f_{k+1} = X e^{i \frac{2\pi}{d}(k+1)} f_k = e^{i \frac{2\pi}{d}} XZ f_k$ □

3.4.3. Állítás. *X, Z uniterek, és $W^*_{a,b} = e^{i \frac{2\pi}{d} ab} W_{-a,-b}$ továbbá $\mathrm{Tr}\, W_{a,b} = d \delta_{a,0} \delta_{b,0}$*

Bizonyítás. $\langle f_l, X f_k \rangle = \langle f_l, f_{k+1} \rangle = \delta_{l,k+1} = \delta_{l-1,k}$, amiből $X^* f_l = f_{l-1}$ $\forall l \in \{0, ..., d-1\}$, azaz $X^* = X^{-1}$, tehát X unitér

Z-re kapjuk, hogy $\langle f_l, Z f_k \rangle = \langle f_l, e^{i \frac{2\pi}{d}} f_k \rangle = e^{i \frac{2\pi}{d}} \langle f_l, f_k \rangle = \langle e^{-i \frac{2\pi}{d}} f_l, f_k \rangle$, azaz $Z^* = Z^{-1}$. Felhasználva, hogy X, Z uniterek és $ZX = e^{i \frac{2\pi}{d}} XZ$:

$W^*_{a,b} = (X^a Z^b)^* = (Z^*)^b (X^*)^a = Z^{d-b} X^{d-a} = e^{i \frac{2\pi}{d}(d-b)(d-a)} X^{d-a} Z^{d-b} = e^{i \frac{2\pi}{d} ab} X^{-a} Z^{-b} = e^{i \frac{2\pi}{d} ab} W_{-a,-b}$

$\mathrm{Tr}\, W_{0,0} = \mathrm{Tr}\, I = d$, tegyük fel, hogy $(a, b) \neq (0, 0)$. Ekkor

$\mathrm{Tr}\, W_{a,b} = \sum_{k=0}^{d-1} \langle f_k, X^a Z^b f_k \rangle = \sum_{k=0}^{d} e^{i \frac{2\pi}{d} kb} \langle f_k, f_{k+a} \rangle$

Ha $a \neq 0$, akkor $\langle f_k, f_{k+a} \rangle = 0$ minden k-ra. Ha $a = 0$, akkor a feltevésünk szerint $b \neq 0$ és így: $\mathrm{Tr}\, W_{a,b} = \sum_{k=0} e^{i \frac{2\pi}{d} kb} = \frac{e^{i \frac{2\pi}{d} bd} - 1}{e^{i \frac{2\pi}{d}} - 1} = 0$ □

3.4.4. Állítás. *$W_{a,b}$, $a,b \in \{0,...,d-1\}$ uniterek és*

$\{\frac{1}{\sqrt{d}}W_{a,b}, a,b \in \{0,...,d-1\}\}$ ortonormált bázist alkot $Lin(\mathscr{H})$-ban a Hilbert-Schmidt skalárszorzatra nézve.

Bizonyítás. Mivel X,Z uniterek, ezért a hatványaik és a szorzatuk is az, így kapjuk, hogy $W_{a,b}$ unitér minden $a,b \in \{0,...,d-1\}$

$W_{a,b}W_{m,n} = X^aZ^bX^mZ^n = e^{i\frac{2\pi}{d}mb}X^{a+m}Z^{n+b}$, és így:

$\langle W_{a,b}, W_{m,n}\rangle_{HS} = \operatorname{Tr} W^*_{a,b}W_{m,n} = \operatorname{Tr} e^{i\frac{2\pi}{d}ab}W_{-a,-b}W_{m,n} = e^{i\frac{2\pi}{d}ab}e^{-i\frac{2\pi}{d}mb}\operatorname{Tr} W_{m-a,n-b} = d\delta_{a,m}\delta_{b,n}$.

$\langle \frac{1}{\sqrt{d}}W_{a,b}, \frac{1}{\sqrt{d}}W_{m,n}\rangle_{HS} = \delta_{a,b}\delta_{m,n}$, amiből kapjuk, hogy $\{\frac{1}{\sqrt{d}}W_{a,b} : a,b \in \{0,...,d-1\}$ ortonormált rendszer, és mivel a számossága $d^2 = \dim Lin(\mathscr{H})$, ezért ortonormált bázis □

3.4.5. Állítás. $\frac{1}{d^2}\sum\limits_{a,b=0}^{d-1} W_{a,b}AW^*_{a,b} = I\frac{\operatorname{Tr} A}{d}$, *$A \in Lin(\mathscr{H})$*

Bizonyítás. Mivel a fenti formula lineáris, ezért elég $Lin(\mathscr{H})$ egy ortonormált bázisán ellenőrizni. Legyen ez $\{|f_i\rangle\langle f_j|\}_{i,j=1}^d$

Így $\sum\limits_{a,b=0}^{d-1} W_{a,b}|f_k\langle|f_l\rangle W^*_{a,b} = \sum\limits_{a,b=0}^{d-1} |W_{a,b}f_k\rangle\langle W_{a,b}f_l| = \sum\limits_{a,b=0}^{d-1} e^{i\frac{2\pi}{d}bk}e^{-i\frac{2\pi}{d}bl}|f_{k+a}\rangle\langle f_{l+a}| = \sum\limits_{a=0}^{d-1}|f_{k+a}\rangle\langle f_{l+a}|\sum\limits_{b=0}^{d-1} e^{i\frac{2\pi}{d}b(k-l)} = \sum\limits_{a=0}^{d-1}|f_{k+a}\rangle\langle f_{l+a}|d\delta_{k,l} = d\delta_{k,l}\sum\limits_{a=0}^{d-1}|f_{k+a}\rangle\langle f_{l+a}| = d\delta_{k,l}I = dI\operatorname{Tr}|f_k\rangle\langle f_l|$ □

3.5. Rényi-divergenciák monotonitási és konvexitási tulajdonságai

3.5.1. Állítás. *f konvex $\Longrightarrow$ D_f együttesen konvex $\mathbb{R}_+^{\mathscr{X}} \times \mathbb{R}_+^{\mathscr{X}}$-en $\forall$ véges $\mathscr{X}$ véges halmazra.*

Bizonyítás. Legyenek $p_i, q_i \in \mathbb{R}_+^{\mathscr{X}}, i \in [r]$, $t_1,...,t_r$ valószínűségeloszlás.

$D_f\left(\sum\limits_{i=1}^r t_ip_i||\sum\limits_{i=1}^r t_iq_i\right) = \sum\limits_{x\in\mathscr{X}} P_f\left(\sum\limits_{i=1}^r t_ip_i(x), \sum\limits_{i=1}^r t_iq_i(x)\right) \le \sum\limits_{x\in\mathscr{X}}\sum\limits_{i=1}^r t_iP_f(p_i(x),q_i(x)) = \sum\limits_{i=1}^r t_i\sum\limits_{x\in\mathscr{X}} P_f(p_i(x),q_i(x)) = D_f(p||q)$ □

3.5.2. Állítás. *f konvex $\implies D_f$ monoton, azaz $\forall \mathscr{X}, \mathscr{Y}$ véges halmazra, $p, q, \in \mathbb{R}_+^{\mathscr{X}}$, $\forall \Phi \in PTP(\mathscr{X}, \mathscr{Y})$: $D_f(\Phi(p)||\Phi(q)) \leq D_f(p||q)$*

Bizonyítás. $\Phi(1_{\{x\}}) = \sum\limits_{y \in \mathscr{Y}} 1_{\{y\}} \Phi_{xy}$, $\Phi_{xy} \geq 0\, \forall x: \sum\limits_{y \in \mathscr{Y}} \Phi_{xy} = 1$ Φ sztochasztikus mátrix.

$\Phi(p) = \sum\limits_y 1_{\{y\}} \sum\limits_x \Phi_{xy} p(x)$

$D_f(\Phi(p)||\Phi(q)) = \sum\limits_y P_f(\sum\limits_x \Phi_{xy} p(x), \sum\limits_x \Phi_{xy} q(x) \leq \sum\limits_{x \in \mathscr{X}} P_f(p(x), q(x)) \sum\limits_{y \in \mathscr{Y}} \Phi_{xy} = D_f(p||q)$

□

Következmény: f konvex: $\implies D_f(p||q) \geq D_f(p(\mathscr{X})||q(\mathscr{X})) = q(\mathscr{X}) f(\frac{p(\mathscr{X})}{q(\mathscr{X})})$.

Speciálisan, ha p, q valószínűségeloszlások: $D_f(p||q) \geq f(1)$

Példa:

$f(t) := \eta(t) = t \log t, f(1) \geq 0 \implies D(p||q) \geq 0\, \forall p, q$ valószínűléségeloszlásra.

$f_\alpha(t) := t^\alpha, \alpha > 1 \implies D_{f_\alpha}(p||q) \geq f_\alpha(1) = 1$

3.5.3. TÉTEL (Monotonitás)**.** *Legyen $\frac{1}{2} \leq \alpha \leq +\infty$ és legyenek $\rho, \sigma \geq 0$. Ekkor bármely teljesen pozitív, nyomtartó ε-ra:*

$D_\alpha^*(\rho||\sigma) \geq D_\alpha^*(\varepsilon(\rho)||\varepsilon(\sigma))$

A fenti tétel szemléletes jelentése, hogy kvantumcsatornákkal hatva az állapotokon, azok távolsága nem nőhet, azaz az állapotok megkülönböztethetősége legfeljebb romolhat.

3.5.4. TÉTEL (Együttes konvexitás)**.** *Legyen $\frac{1}{2} \leq \alpha \leq 1$. Ekkor $D_\alpha^*(\rho||\sigma)$ együttesen konvex ρ, σ nemnegatív operátorokon bármely rögzített $t > 0$-ra, ha $\operatorname{Tr}\rho = t$*

3.5.5. Lemma. *A $(\rho, \sigma) \mapsto \operatorname{Tr}\left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha$ függvény nemnegatív operátorokon konkáv ha $\frac{1}{2} \leq \alpha \leq 1$ és konvex, ha $\alpha > 1$*

Az első tétel bizonyítása a lemmából:

Bizonyítás. A tételt az $\alpha \in [\frac{1}{2}, 1) \cup (1, +\infty)$ esetre bizonyítjuk. Tegyük fel, hogy az alulfekvő Hilbert-tér véges dimenziós. Ha ε teljesen pozitív, nyomtartó leképezés akkor a Stinespring reprezentációs tétel miatt létezik U unitér, hogy:

$$\varepsilon(\gamma) = \operatorname{Tr}_2 U \gamma U^*$$

A reprezentáció miatt elég a parciális nyomra belátni a monotonitást. A **3.4** alfejezet szerint a parciális nyom felírható unitér konjugációk konvex kombinációjaként. A trace ciklikussága miatt az unitér konjugáció nem változtatja meg a Rényi-divergenciát, ezért az együttes konvexitásból következik a monotonitás. □

A második tétel bizonyítása a lemma segítségével:

Bizonyítás. Következik a lemmából, felhasználva, hogy $x \mapsto \log x$ monoton növő és konkáv. □

Ezzel a két tétel bizonyításához már csak a fenti lemmát kell belátnunk. Ennek bizonyítása két összetevőn múlik. Az első ezek közül egy reprezentációs formula $\mathrm{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^{\alpha}$-ra.

3.5.6. Lemma. *Legyenek $\rho, \sigma \geq 0$ operátorok. Ekkor ha $\alpha > 1$, akkor:*

$$\mathrm{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^{\alpha} = \sup_{H\geq 0}(\alpha \,\mathrm{Tr}\, H\rho - (\alpha-1)\,\mathrm{Tr}(H^{\frac{1}{2}}\sigma^{\frac{\alpha-1}{\alpha}}H^{\frac{1}{2}})^{\frac{\alpha}{\alpha-1}}). \tag{3.1}$$

Ugyanez az egyenlőség mondható el az $0 < \alpha < 1$ esetről, ekkor azonban a szuprémum infimumra cserélődik.

A második lemma egy konkavitási eredmény a $\mathrm{Tr}(B^*A^pB)^{\frac{1}{p}}$ kifejezésre.

3.5.7. Lemma. *Egy rögzített B operátorra és bármely A pozitív operátorra az $A \mapsto \mathrm{Tr}(B^*A^pB)^{\frac{1}{p}}$ leképezés konkáv minden $-1 \leq p \leq 1, p \neq 0$-ra.*

3.5.8. Állítás. *Legyen f kétváltozós, együttesen konkáv függvény.*

Ekkor $\sup_x f(x,y)$ y-ban konkáv.

A fenti állítás bizonyításához lásd a [3] könyv **3.5** szakaszát. A **3.5.5.** lemma bizonyítása a **3.5.6.** és **3.5.7.** lemmákból:

Bizonyítás. A **3.5.7.** lemma alapján:

$\sigma \mapsto (1-\alpha)\,\mathrm{Tr}(H^{\frac{1}{2}}\sigma^{\frac{\alpha-1}{\alpha}}H^{\frac{1}{2}})^{\frac{\alpha}{\alpha-1}}$ konkáv $\frac{1}{2} \leq \alpha \leq 1$-re és konvex, ha $\alpha > 1$. Így az állítás adódik a **3.5.6.** lemmában adott reprezentációs formulából. □

Még be kell bizonyítanunk a lemmákat. Az **3.5.6.** lemma bizonyítása:

Bizonyítás. Legyen $\alpha > 1$ és jelöljük β-val a következőt: $\beta := \frac{\alpha-1}{2\alpha}$. Mivel $H^{\frac{1}{2}}\sigma^{2\beta}H^{\frac{1}{2}}$-nak és $\sigma^{\beta}H\sigma^{\beta}$-nak ugyanazok a nemnulla sajátértékei,mivel a **2.4.4** lemma szerint $spec(AB) = spec(BA)$, amiben $A = H^{\frac{1}{2}}\sigma^{\beta}$, $B = \sigma^{\beta}H^{\frac{1}{2}}$ választással adódik az állítás. Így a lemma jobb oldala a következő alakba írható:

$$\sup_{H\geq 0}(\alpha \operatorname{Tr} H\rho - (\alpha-1)\operatorname{Tr}(\sigma^{\beta}H\sigma^{\beta})^{\frac{1}{2\beta}}).$$

Megmutatjuk, hogy a szuprémum értéke $\operatorname{Tr}(\sigma^{-\beta}\rho\sigma^{-\beta})^{\alpha}$. A fenti kifejezés H szerinti deriváltja: $(\alpha \operatorname{Tr} H\rho - (\alpha-1)\operatorname{Tr}(\sigma^{\beta}H\sigma^{\beta})^{\frac{1}{2\beta}})' = \operatorname{Tr} H(\alpha\rho - \frac{\alpha-1}{2\beta}\sigma^{\beta}(\sigma^{\beta}H\sigma^{\beta})^{\frac{1}{2\beta-1}}\sigma^{\beta})$.
Észrevétel:

$\beta = \frac{\alpha-1}{2\alpha} \implies \frac{1}{2\beta} = \frac{\alpha}{\alpha-1}$

$(\alpha\rho - \frac{\alpha-1}{2\beta}\sigma^{\beta}(\sigma^{\beta}H\sigma^{\beta})^{\frac{1}{2\beta-1}}\sigma^{\beta}) = 0$, ha $\alpha\rho = \alpha\sigma^{\beta}(\sigma^{\beta}H\sigma^{\beta})^{\frac{1}{\alpha-1}}\sigma^{\beta}$, amiből $\sigma^{-\beta}\rho\sigma^{-\beta} = (\sigma^{\beta}H\sigma^{\beta})^{\frac{1}{\alpha-1}}$ ahonnan $H = \sigma^{-\beta}(\sigma^{-\beta}\rho\sigma^{-\beta})^{\alpha-1}\sigma^{-\beta}$.

3.5.9. Állítás. *Legyenek X, Y pozitív operátorok, és legyenek $1 < p, q < +\infty$ úgy, hogy $\frac{1}{p} + \frac{1}{q} = 1$.*

Ekkor:

$$\operatorname{Tr} XY \leq \frac{1}{p}\operatorname{Tr} X^p + \frac{1}{q}\operatorname{Tr} Y^q$$

A fenti állítás bizonyításához szükségünk van a következő tételre:

3.5.10. Tétel. *Jelölje $s_k(A)$ az A operátor k. legnagyobb szinguláris értékét. Ekkor:*

$$\sum_{k=1}^{d} s_k(AB) \leq \sum_{k=1}^{d} s_k(A)s_k(B)$$

A tétel bizonyítása megtalálható a könyv IV. fejezetében.

A **3.5.8.** állítás bizonyítása a tételből:

Bizonyítás. A tétel bal oldalán szereplő összegzést elvégezve $\operatorname{Tr}|XY|$-t kapjuk. A tétel jobb oldalán szereplő kifejezésre a Hölder-egyenlőtlenséget alkalmazva kapjuk, hogy

$$\sum_{k=1}^{d} s_k(X)s_k(Y) \leq \sum_{k=1}^{d}\frac{1}{p}s_k(X)^p + \sum_{k=1}^{d}\frac{1}{q}s_k(Y)^q = \frac{1}{p}TrX^p + \frac{1}{q}TrY^q.$$

Ahonnan:

$$|\operatorname{Tr} XY| \leq \operatorname{Tr}|XY| \leq \frac{1}{p} TrX^p + \frac{1}{q} TrY^q$$

□

A fenti állításból adódik, hogy a keresett kifejezés nagyobb vagy egyenlő a szuprémumnál. A derivált nullhelyéből megsejthetjük, hogy hol éretik el a szuprémum. Megmutatjuk, hogy ezt behelyettesítve valóban eléretik a szuprémum. Legyen $H = \sigma^{-\beta}(\sigma^{-\beta}\rho\sigma^{-\beta})^{\alpha-1}\sigma^{-\beta}$. Ekkor

$$\alpha \operatorname{Tr} H\rho - (\alpha - 1)\operatorname{Tr}(\sigma^{\beta} H \sigma^{\beta})^{\frac{1}{2\beta}}$$

$$= \operatorname{Tr}(\sigma^{-\beta}\rho\sigma^{-\beta})^{\alpha}$$

Amiből felhasználva, hogy $\beta = \frac{\alpha-1}{2\alpha}$:

$$= \operatorname{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^{\alpha}$$

,azaz az eredeti állításbeli jobb oldali kifejezés valóban eléri a bal oldali kifejezést.

□

A **3.5.7.** lemma bizonyítása:

3.5.11. Állítás. $p \operatorname{Tr}(B^* A^p B)^{\frac{1}{p}} = \inf_{X \geq 0} (\operatorname{Tr} A^{\frac{p}{2}} B X^{1-p} B^* A^{\frac{p}{2}} - (1-p)\operatorname{Tr} X)$

Ahhoz, hogy ezt belássuk, felhasználjuk a Schatten-féle p-normákra vonatkozó variációs formulákat. A következőkben az alábbi konvencióval élünk:$0^p = 0, p \in \mathbb{R} \setminus \{0\}$. Ennek megfelelően, egy pozitív operátor hatványai csak a tartóján vannak értelmezve, a tartó ortokomplementumán pedig 0-nak definiáljuk.

3.5.12. Lemma. *Legyenek $A, B \in \mathscr{B}(\mathscr{H})_+$ Ekkor*

$$\operatorname{Tr} A^{\alpha} B^{1-\alpha} \leq (\operatorname{Tr} A)^{\alpha} (\operatorname{Tr} B)^{1-\alpha}, \alpha \in [0,1]$$

és ha $A^0 \leq B^0$ *akkor*

$$\operatorname{Tr} A^{\alpha} B^{1-\alpha} \geq (\operatorname{Tr} A)^{\alpha} (\operatorname{Tr} B)^{1-\alpha}, \alpha \in (1, +\infty).$$

Bizonyítás. Legyenek $A = \sum_a a P_a$ és $B = \sum_b b Q_b$ A és B spektrálfelbontásai, és legyenek $c(a,b) := a \operatorname{Tr} P_a Q_b, d(a,b) = b \operatorname{Tr} P_a Q_b$. Ekkor

$$\operatorname{Tr} A^{\alpha} B^{1-\alpha} = \sum_{a,b} a^{\alpha} b^{1-\alpha} \operatorname{Tr} P_a Q_b = \sum_{a,b} c(a,b)^{\alpha} d(a,b)^{1-\alpha}.$$

Legyen $\alpha \in (0,1)$ és $p := \frac{1}{\alpha}, q := \frac{1}{1-\alpha}$. Ekkor $\frac{1}{p} + \frac{1}{q} = 1$ és a Hölder-egyenlőtlenség szerint:

$$\sum_{a,b} c(a,b)^{\alpha} d(a,b)^{1-\alpha} \leq (\sum_{a,b} (c(a,b)^{\alpha})^{p})^{\frac{1}{p}} (\sum_{a,b} (d(a,b)^{1-\alpha})^{\frac{1}{q}}$$

$$= (\sum_{a,b} c(a,b))^{\alpha} (\sum_{a,b} d(a,b))^{1-\alpha}$$

$$= (\mathrm{Tr} A)^{\alpha} (\mathrm{Tr} B)^{1-\alpha},$$

ami bizonyítja a lemmát $\alpha \in (0,1)$-re, és az $\alpha = 0, \alpha = 1$ esetek nyilvánvalóak. Legyen $\alpha \in (1,+\infty)$ és legyen $p := \frac{1}{\alpha}, q := \frac{1}{1-\alpha}$. Ekkor $\frac{1}{p} + \frac{1}{q} = 1$, és $p > 0, q < 0$, valamint $A^0 \leq B^0$ amiből következik, hogy ha $d(a,b) = 0$ valamely a,b-re akkor $c(a,b) = 0$. Így a fordított Hölder-egyenlőtlenségből következik, hogy:

$$\sum_{a,b} c(a,b)^{\alpha} d(a,b)^{1-\alpha} \geq (\sum_{a,b} (c(a,b)^{\alpha})^{p})^{\frac{1}{p}} (\sum_{a,b} (d(a,b)^{1-\alpha})^{q})^{1-\alpha})^{\frac{1}{q}}$$

$$= (\mathrm{Tr} A)^{\alpha} (\mathrm{Tr} B^{1-\alpha}),$$

ami bizonyítja a lemma másik felét. □

3.5.13. Állítás. *Bármely $C \in \mathscr{B}(\mathscr{H})_+$ és $p \in \mathbb{R} \setminus \{0\}$ esetén a következők igazak:*

$$||C||_p := (\mathrm{Tr} C^p)^{\frac{1}{p}} = \begin{cases} \sup\limits_{\sigma \in S(\mathscr{H})} \mathrm{Tr} C \sigma^{1-\frac{1}{p}}, & \text{ha } p \in [1,+\infty) \\ \inf\limits_{\sigma \in S(\mathscr{H}), C^0 \leq \sigma^0} \mathrm{Tr} C \sigma^{1-\frac{1}{p}}, & \text{ha } p \in (0,1) \\ \inf\limits_{\sigma \in S(\mathscr{H}), C^0 \geq \sigma^0} \mathrm{Tr} C \sigma^{1-\frac{1}{p}} & \text{ha } p \in (-\infty,0) \end{cases}$$

Bizonyítás. Legyen $p \in [1,+\infty)$, $\alpha := \frac{1}{p} \in (0,1)$, és $A := C^p = C^{\frac{1}{\alpha}}$. Ekkor az előző lemma első feléből adódik, hogy bármely $B \in \mathscr{B}(\mathscr{H})_+$ esetén:

$$\mathrm{Tr} C B^{1-\alpha} = \mathrm{Tr} A^{\alpha} B^{1-\alpha} \leq (\mathrm{Tr} A)^{\alpha} (\mathrm{Tr} B)^{1-\alpha},$$

és így:

$$(\mathrm{Tr} C^p)^{\frac{1}{p}} \geq \mathrm{Tr} C (\frac{B}{\mathrm{Tr} B})^{1-\alpha} = \mathrm{Tr} C (\frac{B}{\mathrm{Tr} B})^{1-\frac{1}{p}}.$$

Amiből adódik, hogy:

$$(\mathrm{Tr} C^p)^{\frac{1}{p}} \geq \sup_{\sigma \in S(\mathscr{H})} \mathrm{Tr} C \sigma^{1-\frac{1}{p}},$$

és egyenlőség akkor teljesül, ha $\sigma = \frac{C^p}{\mathrm{Tr}\, C^p}$.

A következőkben legyen $p \in (0,1), \alpha := \frac{1}{p} \in (1,+\infty)$, és $A := C^p = C^{\frac{1}{\alpha}}$. Ekkor bármely $B \in \mathscr{B}(\mathscr{H})_+$-ra amire $A^0 \le B^0$ a fenti egyenlőtlenségek az ellenkező irányban teljesülnek, és így

$$(\mathrm{Tr}\, C^p)^{\frac{1}{p}} \le \inf_{\sigma \in S(\mathscr{H})} \mathrm{Tr}\, C\sigma^{1-\frac{1}{p}}.$$

Egyenlőség ismét akkor vétetik fel, ha $\sigma = \frac{C^p}{\mathrm{Tr}\, C^p}$. Végül legyen $p \in (-\infty, 0), \alpha := 1 - \frac{1}{p} \in (1,+\infty)$, és $B := C^p = C^{\frac{1}{1-\alpha}}$. Ekkor bármely $A \in \mathscr{B}(\mathscr{H})_+$-ra amire $A^0 \le C^0 = B^0$ tudjuk, hogy

$$\mathrm{Tr}\, A^\alpha C = \mathrm{Tr}\, A^\alpha B^{1-\alpha} \ge (\mathrm{Tr}\, A)^\alpha (\mathrm{Tr}\, B)^{1-\alpha} = (\mathrm{Tr}\, A)^\alpha (\mathrm{Tr}\, C^p)^{\frac{1}{p}},$$

és így,

$$(\mathrm{Tr}\, C^p)^{\frac{1}{p}} \le \mathrm{Tr}\, C\left(\frac{A}{\mathrm{Tr}\, A}\right)^\alpha = \mathrm{Tr}\, C\left(\frac{A}{\mathrm{Tr}\, A}\right)^{1-\frac{1}{p}}$$

Ebből kapjuk, hogy

$$(\mathrm{Tr}\, C^p)^{\frac{1}{p}} \le \inf_{\sigma \in S(\mathscr{H}), C^0 \ge \sigma^0} \mathrm{Tr}\, C\sigma^{1-\frac{1}{p}},$$

és az egyenlőséget $\sigma := \frac{C^{\frac{1}{1-\alpha}}}{\mathrm{Tr}\, C^{\frac{1}{1-\alpha}}}$ választással érhetjük el. □

3.5.14. Állítás. *Bármely $C \in \mathscr{B}(\mathscr{H})_+$ és $p \in \mathbb{R} \setminus \{0\}$ esetén igazak a következők:*

$$\mathrm{Tr}\, C^p = \begin{cases} \sup\limits_{X \in \mathscr{B}(\mathscr{H})_+} \{p\, \mathrm{Tr}\, CX^{1-\frac{1}{p}} - (p-1)\, \mathrm{Tr}\, X\} & \text{ha } p \in [1,+\infty) \\ \inf\limits_{X \in \mathscr{B}(\mathscr{H})_+, C^0 \le X^0} \{p\, \mathrm{Tr}\, CX^{1-\frac{1}{p}} - (p-1)\, \mathrm{Tr}\, X\} & \text{ha } p \in (0,1) \\ \sup\limits_{X \in \mathscr{B}(\mathscr{H})_+, C^0 \ge X^0} \{p\, \mathrm{Tr}\, CX^{1-\frac{1}{p}} - (p-1)\, \mathrm{Tr}\, X\} & \text{ha } p \in (-\infty, 0) \end{cases}$$

Bizonyítás. Az állítást a $p \in [1,+\infty)$ esetre bizonyítjuk, a bizonyítás a többi esetben hasonlóan történik. Ekkor

$$\sup_{X \in \mathscr{B}(\mathscr{H})_+} \{p\, \mathrm{Tr}\, CX^{1-\frac{1}{p}} - (p-1)\, \mathrm{Tr}\, X\} = \sup_{\sigma \in S(\mathscr{H})} \sup_{\lambda > 0} f(\lambda),$$

ahol

$$f(\lambda) := p\lambda^{1-\frac{1}{p}}\, \mathrm{Tr}\, C\sigma^{1-\frac{1}{p}} - (p-1)\lambda$$

konkáv.$f'(\lambda) = (p-1)\lambda^{-\frac{1}{p}}\operatorname{Tr} C\sigma^{1-\frac{1}{p}} - (p-1)$, ami pontosan akkor 0, ha $\lambda = \lambda_p = (\operatorname{Tr} C\sigma^{1-\frac{1}{p}})^p$, és

$$f(\lambda_p) = p(\operatorname{Tr} C\sigma^{1-\frac{1}{p}})^{p-1}\operatorname{Tr} C\sigma^{1-\frac{1}{p}} - (p-1)(\operatorname{Tr} C\sigma^{1-\frac{1}{p}})^p = (\operatorname{Tr} C\sigma^{1-\frac{1}{p}}).$$

Így,

$$\sup_{\sigma\in S(\mathscr{H})}\sup_{\lambda>0} f(\lambda) = \sup_{\sigma\in S(\mathscr{H})}(\operatorname{Tr} C\sigma^{1-\frac{1}{p}})^p = \operatorname{Tr} C^p,$$

ahol az utolsó egyenlőség az előző lemmából következik. □

A fentiek alapján a reprezentációs formula a következőképpen bizonyítható:

Bizonyítás. Legyen $C = B^*A^pB$, ekkor a fenti állítás alapján minden $-1 \le p \le 0$-ra:

$\operatorname{Tr} C^{\frac{1}{p}} = \sup_{X\ge 0} \frac{1}{p}\operatorname{Tr} CX^{1-p} - (\frac{1}{p}-1)\operatorname{Tr} X$

Mivel p nempozitív, ezért:

$p\operatorname{Tr} C^{\frac{1}{p}} = \inf_{X\ge 0}\operatorname{Tr} CX^{1-p} - (1-p)\operatorname{Tr} X$

Amiből C definíciója szerint:

$p\operatorname{Tr}(B^*A^pB)^{\frac{1}{p}} = \inf_{X\ge 0}\operatorname{Tr} B^*A^pBX^{1-p} - (1-p)\operatorname{Tr} X$ ahonnan felhasználva a nyom ciklikusságát kapjuk, hogy

$p\operatorname{Tr}(B^*A^pB)^{\frac{1}{p}} = \inf_{X\ge 0}\operatorname{Tr} A^{\frac{p}{2}}BX^{1-p}B^*A^{\frac{p}{2}} - (1-p)\operatorname{Tr} X$, ami éppen a bizonyítandó állítás.

□

Ha be tudjuk látni, hogy $(A,X)\mapsto \operatorname{Tr} A^{\frac{p}{2}}BX^{1-p}B^*A^{\frac{p}{2}}$ együttesen konvex nemnegatív operátorokon, akkor $p\operatorname{Tr}(B^*A^pB)^{\frac{1}{p}}$ együttesen konvex függvények infimuma, ami konvex, ez pedig bizonyítaná a lemmát. Ahhoz, hogy ezt belássuk írjuk a fenti kifejezést a következő alakba:

Bizonyítás. $\operatorname{Tr} A^{\frac{p}{2}}BX^{1-p}B^*A^{\frac{p}{2}} = \operatorname{Tr} Z^pK^*Z^{1-p}K$, ahol

$$\mathbf{K} = \begin{pmatrix} 0 & 0 \\ B^* & 0 \end{pmatrix},\ \mathbf{Z} = \begin{pmatrix} A & 0 \\ X & 0 \end{pmatrix}$$

K-ra, ami egy operátor $\mathscr{H} \oplus \mathscr{H}$-ban, tekinthetünk úgy mint egy vektorra $(\mathscr{H} \oplus \mathscr{H}) \otimes (\mathscr{H} \oplus \mathscr{H})$-ban, és jelölhetjük ezt a vektort $\overline{K}$-val.

Így $\operatorname{Tr} Z^p K^* Z^{1-p} K = \langle \overline{K}, Z^p \otimes Z^{1-p} \overline{K} \rangle$.

3.5.15. TÉTEL (Ando konvexitási tétele)**.** *Bármely K $m \times n$-es mátrixra és minden $1 \leq q \leq 2$ és $0 \leq r \leq 1$, ahol $q - r \geq 1$ az $(A, B) \mapsto \operatorname{Tr}(K^* A^q K B^{-r})$ konvex $\mathscr{B}(\mathscr{H}) \times \mathscr{B}(\mathscr{H}) \mapsto \mathbb{R}$-en.*

A bizonyítás megtalálható az [1] cikkben. Az előbbi tétel alapján a fenti egyenlőség jobb oldala Z-nek konvex függvénye, ami ekvivalens azzal, hogy $(A, X) \mapsto \operatorname{Tr} A^{\frac{p}{2}} B X^{1-p} B^* A^{\frac{p}{2}}$ együttesen konvex. $\square$

4. fejezet

Állapotok klónozása és megosztása

Az alábbi fejezetben a Rényi-divergenciák monotonitásának egy alkalmazását vizsgáljuk meg. Ez a fejezet a [11] könyvre és a [9] jegyzetre támaszkodik.

4.0.1. Definíció. Az $S \subseteq S(\mathscr{H})$ állapotok halmaza **klónozható**, ha

$\exists \Phi \in CPTP(\mathscr{H}, \mathscr{H} \otimes \mathscr{H})$, amire $\Phi(\rho) = \rho \otimes \rho \ \forall \rho \in S$,

megosztható, ha $\exists \Phi \in CPTP(\mathscr{H}, \mathscr{H} \otimes \mathscr{H})$, amire

$\mathrm{Tr}_2 \Phi(\rho) = \mathrm{Tr}_1 \Phi(\rho) = \rho, \forall \rho \in S$

4.0.2. Állítás. *A klónozhatóság és megoszthatóság tulajdonságai*

1, *S klónozható* $\implies$ *S megosztható*

2, *A teljes állapottér nem klónozható, sőt, ha S tartalmaz nemtriviális szakaszt akkor nem klónozható.*

3, *Ha* $\forall \rho, \sigma \in S$*:*$\rho \perp \sigma \implies$ *S klónozható*

Bizonyítás.

1, Ha S klónozható, akkor $\mathrm{Tr}_2 \Phi(\rho) = \rho \, \mathrm{Tr}\, \rho = \rho = \mathrm{Tr}_1 \Phi(\rho)$

2, Következik abból, hogy a $\rho \mapsto \rho \otimes \rho$ leképezés nem affin.

3, Legyen $S = \{\rho_1, ..., \rho_r\}$ olyan, hogy $\rho_i \perp_{i \neq j} \rho_j$. Legyen $P := I - \sum_{i=1}^{r} \rho_i^0$ és minden $n \in \mathbb{N}$-re:

$$\Phi_n(X) := \sum_{i=1}^{r} (\mathrm{Tr} X \rho_i^0) \rho_i^{\otimes n} + (\mathrm{Tr} X P) \sigma_n,\ X \in Lin(\mathscr{H}),$$

ahol $\sigma_n \in S(\mathscr{H}^{\otimes n})$ rögzített sűrűségoperátor. Ekkor Φ_n CPTP és $\Phi_n(\rho_i) = \rho_i^{\otimes n}$ minden i-re.

□

4.0.3. TÉTEL. *S klónozható* $\iff \forall \rho, \sigma\ \rho \neq \sigma : \rho \perp \sigma$

Bizonyítás. $\Leftarrow$-t láttuk az előző állításban.

$\Rightarrow$-hoz legyen $\alpha \in (\frac{1}{2}, 1)$. Ekkor minden ρ, σ, Φ-re

$$D_\alpha(\Phi(\rho)||\Phi(\sigma)) = \frac{1}{\alpha - 1} \log \mathrm{Tr} \Phi(\rho)^\alpha \Phi(\sigma)^{1-\alpha} \leq D_\alpha(\rho||\sigma).$$

Legyen $Q_\alpha(\Phi(\rho)||\Phi(\sigma)) := \mathrm{Tr} \Phi(\rho)^\alpha \Phi(\sigma)^{1-\alpha}$. Tegyük fel, hogy $\{\rho, \sigma\}$ klónozható.

$$Q_\alpha(\Phi(\rho)||\Phi(\sigma)) \geq Q_\alpha(\rho||\sigma)$$

, de Φ klónozási operáció:

$$Q_\alpha(\rho^{\otimes 2}||\sigma^{\otimes 2}) = Q_\alpha(\rho||\sigma)^2$$

$$0 \leq Q_\alpha(\rho||\sigma) \leq 1 \implies Q_\alpha = 0 \iff \rho \perp \sigma$$

és

$$Q_\alpha(\rho||\sigma) = 1 \iff \rho = \sigma.$$

□

Következmény: (nemklónozhatósági tétel)

Egy legalább kétdimenziós kvantumrendszer tiszta állapotainak halmaza nem klónozható.

Irodalomjegyzék

[1] T.Ando, Convexity of certain maps on positive definite matrices and applications to Hadamard products, *Linear Algebra Appl.* **26**, 203-241 (1979)

[2] Rajendra Bhatia, Matrix Analysis, Springer (1997)

[3] S.Boyd, L.Vandenberghe, Convex Optimization, Cambridge University Press, (2004)

[4] I.Csiszár, Information type measure of difference of probability distributions and indirect observations, *Stud.Sci.Math.Hung.* **2** (1967) 299-318.

[5] Rupert L. Frank, Elliott H. Lieb, Monotonicity of a relative Rényi entropy, *Journal of Mathematical Physics* **54**, 122203 (2013)

[6] F.Hiai, Matrix analysis:Matrix monotone functions, matrix means, and majorization, *Interdiscip.Inf.Sci.* **16** 139248 (2010)

[7] F.Hiai, M.Mosonyi, D.Petz, C.Bény, Quantum f-divergences and error correction, *Reviews in Mathematical Physics* **23** 691 (2011)

[8] E. H. Lieb and W. Thirring, Inequalities for the moments of the Schrödinger Hamiltonian and their relation to Sobolev inequalities, in Studies in Mathematical Physics:*Essays in Honor of Valentine Bergman,* edited by E. H. Lieb, B. Simon, and A. S. Wightman (Princeton University Press, Princeton, 1976), pp. 269-297

[9] M.Mosonyi Quantum information theory, unpublished lecture notes

[10] M. Müller-Lennert et al., "On quantum Rényi entropies: a new definition, some properties", *J.Maths. Phys.* **54,** 122203 (2013)

[11] M.A. Nielsen, I.L.Chuang, Quantum computation and Quantum information, Cambridge University Press, (2000)

[12] D.Petz, Quasi-entropies for states of a von Neumann algebra, *Publ. RIMS. Kyoto Univ.* **21** (1985) 781-800.

[13] D.Petz, Quasi-entropies for finite quantum systems, *Rep.Math.Phys.* **23** (1986) 57-65.

[14] A.Rényi, On measures of information and entropy, *Proceedings of the fourth Berkeley Symposium on Mathematics, Statistics and Probability 1960.* pp. 547-561.

[15] W. F. Stinespring, "Positive functions on C*-algebras," *Proc.Am.Math.Soc.* **6**, 211-216 (1955)

[16] David Sutter, Mario Berta, Marco Tomamichel, Multivariate trace inequalities, 2017, *Communications in Mathematical Physics*

[17] M.M.Wilde, A.Winter, and D.Yang, Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy, *Comm.Math.Phys.* 331 **2** 593622 (2014)