Ez a jegyzet a 2014/2015 tanév őszi félévében a BME-n tartott *Kvantum csatornák* előadás alapján készült. Talán helyesebb lenne definíciók, tételek és bizonyítások gyűjteményének nevezni, mivel magyarázatokat csak rendkívül vázlatos formában tartalmaz.

Tervben van egy (jelentősen) bővített változat elkészítése is, amelyben a tananyagon túlmutató tartalom mellett az olvasó több magyarázatot és példát találhat, és (remélhetőleg) kevesebb hibát. Mindenféle észrevételt szívesen veszek.

Vrana Péter

Tartalomjegyzék

1. Kvantummechanika alapjai

- kvantumfizika: fizikai elméletek általános kerete
- véletlen eseményekkel foglalkozik, matematikailag a valószínűségszámítás általánosításának tekinthető
- Hilbert-teres megfogalmazás:
  - kvantummechanikai rendszer $\rightsquigarrow$ szeparábilis Hilbert-tér $\mathcal{H}$
  - obszervábilisek: $\mathcal{B}(\mathcal{H})$ önadjungált (vagy normális) elemei
  - állapotok: $\mathcal{S}(\mathcal{H}) = \{\varrho \in \mathcal{T}(\mathcal{H}) | \varrho \geq 0, \operatorname{Tr} \varrho = 1\}$ elemei
  - $A \in \mathcal{B}(\mathcal{H})$ m. momentuma a $\varrho \in \mathcal{T}(\mathcal{H})$ állapotban $\operatorname{Tr}(\varrho A^m) \rightsquigarrow$ valószínűségi mérték A spektrumán
  - speciálisan: A várható értéke $\operatorname{Tr}(\varrho A^m)$

- „összetett rendszer” Hilbert-tere a részekhez tartozó Hilbert-terek tenzorszorzata, az egyik rész egy obszervábilisét a többi identitásával tenzorszorozva kapjuk a megfelelő obszervábilist az egész rendszeren
- zárt rendszer állapota az időben $t \mapsto e^{-iHt}\varrho e^{iHt}$ módon változik, ahol $H = H^*$ neve Hamilton-operátor, a klasszikus energiához tartozó obszervábilis (esetleg nem korlátos)
- tfh $\{|i\rangle\}_{i\in I}$ ortonormált bázis és $(a_i)_{i\in I}$ különböző számok családja, az $A = \sum_{i\in I} a_i|i\rangle\langle i|$ obszervábilis mérése után az állapot a $|i\rangle\langle i|$ állapotok valamelyike (Neumann-féle mérés)

• egy adott kísérlet (jelenség) elméleti leírásához választunk egy alkalmas Hilbert-teret, a preparációnak megfelelő állapotot és a mérésnek megfelelő obszervábilist

1.1. Állítás. *Legyen $\mathcal{H}$ Hilbert-tér, $A \in \mathcal{B}(\mathcal{H})$ normális, $\varrho \in \mathcal{S}(\mathcal{H})$. Ekkor létezik pontosan egy μ Borel valószínűségi mérték $\mathbb{C}$-n, amelyre*

$$\int_{\mathbb{C}} z^m \overline{z}^n d\mu(z) = \mathrm{Tr}\left(\varrho A^m A^{*n}\right) \tag{1.1}$$

teljesül. Továbbá $\mathrm{supp}\,\mu \subseteq \mathrm{spec}(A)$.

Bizonyítás. Legyen $E : \mathrm{B}(\mathbb{C}) \to \mathcal{B}(\mathcal{H})$ az A spektrális mértéke, azaz

$$A = \int_{\mathbb{C}} z dE(z) \tag{1.2}$$

Ekkor $\mu(B) := \mathrm{Tr}(\varrho E(B))$ valószínűségi mérték $\mathbb{C}$-n, $\mathrm{supp}\,\mu \subseteq \mathrm{supp}\,E = \mathrm{spec}(A)$, és

$$\int_{\mathbb{C}} z^m \overline{z}^n d\mu(z) = \mathrm{Tr}\left(\varrho \int_{\mathbb{C}} z^m \overline{z}^n dE(z)\right) = \mathrm{Tr}\left(\varrho A^m A^{*n}\right) \tag{1.3}$$

Az egyértelműség abból következik, hogy a valós polinomokkal kompakt tartományon egyenletesen approximálható minden folytonos függvény. □

Megjegyzés. Ha $A = A^*$, akkor μ tartója $\mathbb{R}$ része.

Megjegyzés. A konstrukció értelmes akkor is, ha A nem korlátos, persze a momentumok létezésére ekkor nincs garancia.

1. HF. Legyen $\mathcal{H} = L^2(\mathbb{R}, \lambda)$, ahol λ a Lebesgue-mérték. A $(Qf)(x) = xf(x)$ és $(Pf)(x) = -if'(x)$ definíciók önadjungált operátorokat határoznak meg (pl. kompakt tartójú sima függvények terén értelmesek, ez sűrű), hasonlóan $H = \frac{P^2}{2} + \frac{Q^2}{2}$ is. Jelölje $|\psi\rangle$ a $\psi(x) = \pi^{-1/4}e^{-x^2/2}$ módon adott függvényt. Ellenőrizzük, hogy $|\psi\rangle\langle\psi|$ állapot, és határozzuk meg Q illetve H eloszlását ebben az állapotban.

1.2. Definíció. $\varrho \in \mathcal{S}(\mathcal{H})$ *tiszta*, ha nem áll elő állapotok nemtriviális konvex kombinációjaként.

1.3. Állítás. *$\varrho \in \mathcal{S}(\mathcal{H})$ pontosan akkor tiszta, ha 1 rangú projektor.*

Bizonyítás. Ha $\varrho_1, \varrho_2 \geq 0$ és $0 < \alpha < 1$, akkor $\ker(\alpha\varrho_1 + (1-\alpha)\varrho_2) = \ker \varrho_1 \cap \ker \varrho_2$, tehát az 1 rangú projektorok tiszták. Ha viszont ϱ nem 1 rangú, akkor a spektrálfelbontása állapotok nemtriviális konvex kombinációjaként állítja elő. □

- további általánosítás célszerű: $\mathcal{B}(\mathcal{H})$ helyett annak egy (normában zárt) rész-*-algebráját választhatjuk obszervábiliseknek (pl. lehetnek kísérletileg hozzáférhetetlen mennyiségek), illetve $\mathcal{S}(\mathcal{H})$ helyett annak egy konvex részhalmazát választhatjuk állapotoknak (pl. nem minden elem valósítható meg preparációval)

1.4. Példa. (klasszikus) valószínűségelmélet megszámlálható eseménytéren: Ω véges vagy megszámlálható halmaz, $\mathcal{H} = \ell^2(\Omega)$ egy ortonormált bázisa $\{|\omega\rangle\}_{\omega\in\Omega}$. Minden korlátos $\Omega \to \mathbb{C}$ függvény meghatároz egy $M_f \in \mathcal{B}(\mathcal{H})$ operátort $(M_f a)(\omega) = f(\omega)a(\omega)$ módon. $M_f \in \mathcal{T}(\mathcal{H})$ pontosan akkor, ha

$$\exists \operatorname{Tr} M_f = \sum_{\omega\in\Omega} \langle\omega|M_f|\omega\rangle \text{ azaz } \sum_{\omega\in\Omega} |f(\omega)| < \infty \tag{1.4}$$

$M_f \geq 0$ pontosan akkor, ha $\forall\omega : f(\omega) \geq 0$, tehát $M_f \in \mathcal{S}(\mathcal{H})$ akkor teljesül, ha f egy diszkrét eloszlás elemi eseményeinek valószínűségeiből áll.

Megjegyzés. Egy $\mathcal{A}$ Banach-*-algebrát C^*-algebrának nevezünk, ha $\forall A \in \mathcal{A}$: $\|AA^*\| = \|A\|^2$. Ez mindig izomorf egy Hilbert-tér feletti korlátos operátorok egy normában zárt rész-*-algebrájával. Megfordítva: $\mathcal{B}(\mathcal{H})$ normában zárt rész-*-algebrája az operátornormával C^*-algebra.

Megjegyzés. Tekinthetjük az $\mathcal{A}$ C^*-algebrát is alapvető objektumnak, ekkor állapotnak nevezzük az $\omega : \mathcal{A} \to \mathbb{C}$ pozitív, 1 normájú lineáris funkcionálokat. Adott $(\mathcal{A}, \omega)$ esetén létezik olyan $\mathcal{H}$ Hilbert-tér, $\Omega \in \mathcal{H}$ és $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ izometrikus *-algebra-homomorfizmus, amivel $\forall A \in \mathcal{A} : \omega(A) = \operatorname{Tr} |\Omega\rangle\langle\Omega|\pi(A)$

1.5. Példa. Legyen X lokálisan kompakt Hausdorff tér, $C_0(X)$ a folytonos, végtelenben eltűnő komplex értékű függvények halmaza, a pontonkénti műveletekkel és a szuprémumnormával ez C^*-algebra. Ha $\mathbb{P}$ valószínűségi Borel-mérték X-en, akkor meghatároz egy állapotot

$$f \mapsto \int_X f d\,\mathbb{P} \tag{1.5}$$

módon.

- mostantól a szereplő Hilbert-terek véges dimenziósak lesznek, $\mathcal{X}, \mathcal{Y}, \ldots$ véges halmazok, a szereplő C^*-algebrák pedig valamilyen $\mathcal{B}(\mathcal{H})$ rész-*-algebrái

1.6. Állítás. *Ha $\mathcal{A} \leq \mathcal{B}(\mathcal{H})$ rész-*-algebra, akkor C^*-algebra, és mind a topologikus, mind az algebrai duálisa $\mathcal{A}$-val azonosítható a $(\varrho, A) \mapsto \operatorname{Tr}(\varrho A)$ párosításon keresztül.*

Bizonyítás. $\dim \mathcal{A} \leq (\dim \mathcal{H})^2 < \infty$ miatt zárt altér, tehát Banach-*-algebra, a C*-tulajdonság érvényben marad. Emellett a kétféle duális megegyezik (mint vektorterek). A $(\varrho, A) \mapsto \operatorname{Tr}(\varrho A)$ leképezés bilineáris és nemelfajuló, mert $\operatorname{Tr} A^*A > 0$ ha $A \neq 0$. □

1.7. Állítás. *A fenti azonosítás szerint a $\mathcal{B}(\mathcal{H})$ normált tér duálisa $\mathcal{T}(\mathcal{H})$.*

Bizonyítás.

$$|\operatorname{Tr} XA| \leq \operatorname{Tr}|XA| = \operatorname{Tr}\sqrt{XAA^*X^*} \leq \operatorname{Tr}\sqrt{X\,\|AA^*\|\,X^*} = \|A\|\,\|X\|_1 \tag{1.6}$$

Ha $X \in \mathcal{B}(\mathcal{H})$ polárfelbontása $X = UR$, akkor

$$\sup_{\|A\| \leq 1} |\operatorname{Tr} XA| \geq |\operatorname{Tr} XU^*| = |\operatorname{Tr} U^*UR| = \operatorname{Tr} R = \|X\|_1 \tag{1.7}$$

□

Megjegyzés. A fenti U^* az X által generált C*-algebrában van.

- ha $\mathcal{X}$ halmaz, $\ell^p(\mathcal{X})$ jelöli a $\mathbb{C}^{\mathcal{X}}$ vektorteret a p-normával, ezt mindig $\mathcal{B}(\mathbb{C}^{\mathcal{X}})$ diagonális mátrixokból álló alterével azonosítjuk, a norma a megfelelő Schatten-norma leszűkítése
- speciálisan: $\ell^1(\mathcal{X}) \leq \mathcal{T}(\mathbb{C}^{\mathcal{X}})$
- $\mathcal{B}(\mathcal{H} \otimes \mathcal{K}) \simeq \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{K})$
- ha $\varrho \in \mathcal{S}(\mathcal{H} \otimes \mathcal{K})$ egy összetett rendszer állapota, de egy $A \in \mathcal{B}(\mathcal{H})$ obszervábilis várható értékére vagyunk kíváncsiak, azt megkaphatjuk $\operatorname{Tr} \varrho(A \otimes \mathrm{id}_{\mathcal{K}})$ módon
- másik lehetőség: az $A \mapsto \operatorname{Tr} \varrho(A \otimes \mathrm{id}_{\mathcal{K}})$ lineáris leképezést reprezentáló elemet tekintjük $\mathcal{T}(\mathcal{H})$-ban, ez egy állapot lesz

1.8. Definíció. Legyen $X \in \mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Azt a $\operatorname{Tr}_B X \in \mathcal{T}(\mathcal{H}_A)$ elemet, amelyre minden $A \in \mathcal{B}(\mathcal{H}_A)$ esetén $\operatorname{Tr}(\operatorname{Tr}_B X)A = \operatorname{Tr} X(A \otimes \mathrm{id}_{\mathcal{H}_B})$ teljesül, az X marginálisának (redukált állapot) nevezzük.

1.9. Állítás. *Ha $X \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, akkor $\operatorname{Tr}_B X \in \mathcal{S}(\mathcal{H}_A)$.*

Bizonyítás. Ha $A \geq 0$ tetszőleges, akkor $A \otimes \mathrm{id}_{\mathcal{H}_B} \geq 0$ és így $\operatorname{Tr}(\operatorname{Tr}_B X)A = \operatorname{Tr} X(A \otimes \mathrm{id}_{\mathcal{H}_B}) \geq 0$, tehát $\operatorname{Tr}_B X \geq 0$. Másrészt $\operatorname{Tr}(\operatorname{Tr}_B X) = \operatorname{Tr} X(\mathrm{id}_{\mathcal{H}_A} \otimes \mathrm{id}_{\mathcal{H}_B}) = \operatorname{Tr} X$. □

- jelölés: a részrendszereket $A, B, C, \ldots$ betűkkel cimkézzük, ezek egy részhalmazához tartozó Hilbert-teret pl. $\mathcal{H}_{ABD}$ módon jelöljük, ha pl. $\varrho \in \mathcal{S}(\mathcal{H}_{ABCD})$, akkor $\operatorname{Tr}_B \varrho = \varrho_{ACD}$ a szokásos jelölés, $\varrho_{ABCD} = \varrho$.

- zárt rendszer állapota az időben $\varrho \mapsto U\varrho U^*$ módon változik, ahol U unitér operátor
- ha a rendszer nem zárt, egy nagyobb rendszer részeként tekinthetünk rá, ami esetleg már (közelítőleg) zárt
- ennek megfelelően fizikai folyamatok modelljének tekinthetjük a $\varrho_A \mapsto \operatorname{Tr}_E U(\varrho \otimes \varrho_E)U^*$ alakú leképezéseket is, ahol $U : \mathcal{H}_{AE} \to \mathcal{H}_{AE}$ unitér
- még általánosabban: a bemeneti és kimeneti Hilbert-terek különbözőek is lehetnek

1.10. Definíció. Egy $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ lineáris leképezés pozitív, ha $X \geq 0$ esetén $T(X) \geq 0$. T teljesen pozitív, ha $\forall n \in \mathbb{N} : T \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}$ pozitív.

1.11. Állítás. *Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ lineáris leképezés. Ekkor a következők ekvivalensek:*

1. *T teljesen pozitív*
2. *$T(\varrho) = \sum_{j=1}^r K_j \varrho K_j^*$ valamely $K_j : \mathcal{H}_A \to \mathcal{H}_B$ lineáris leképezésekre (Kraus-reprezentáció)*
3. *$T(\varrho) = \operatorname{Tr}_E U\varrho U^*$ valamely $U : \mathcal{H}_A \to \mathcal{H}_{BE}$ lineáris leképezésre (Stinespring-reprezentáció)*

Ha ezek teljesülnek, T pontosan akkor trace-őrző, ha U izometria, illetve ha $\sum_{i=j}^r K_j^* K_j = \mathrm{id}_{\mathcal{H}_A}$.

Bizonyítás. **1 $\Longrightarrow$ 2** Legyen $\{|i\rangle\}_{i\in I}$ a $\mathcal{H}_A$ egy bázisa, $\Phi = \sum_{i,i'\in I} |i\rangle\langle i'| \otimes |i\rangle\langle i'| \in \mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_A)$. Tekintsük a $(T \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_A)})(\Phi)$ pozitív operátor egy $\sum_{j=1}^r |\psi_j\rangle\langle\psi_j|$ dekompozícióját. Ekkor $|\psi_j\rangle = (K_j \otimes \mathrm{id}_{\mathcal{H}_A}) \sum_{i\in I} |i\rangle \otimes |i\rangle$ teljesül valamilyen $K_j : \mathcal{H}_A \to \mathcal{H}_B$ lineáris leképezésekre, tehát

$$(T \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_A)})(\Phi) = \sum_{i=1}^r (K_j \otimes \mathrm{id}_{\mathcal{H}_A})\Phi(K_j \otimes \mathrm{id}_{\mathcal{H}_A})^* \tag{1.8}$$

teljesül. Mivel a $T \mapsto (T \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_A)})(\Phi)$ lineáris leképezés injektív, T a fenti alakú.

2 $\Longrightarrow$ 3 Legyen $\mathcal{H}_E = \mathbb{C}^r$, $U\psi = \sum_{j=1}^r K_j\psi \otimes |j\rangle$. Ekkor

$$\operatorname{Tr}_E U\varrho U^* = \sum_{j,j'=1}^r K_j \varrho K_{j'}^* \operatorname{Tr} |j\rangle\langle j'| = \sum_{j=}^r K_j \varrho K_j^* \tag{1.9}$$

3 $\Longrightarrow$ 1 Legyen $U : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ izometria. Ekkor a $T : \varrho \mapsto \operatorname{Tr}_E U\varrho U^*$ leképezés lineáris és pozitív, mert $\varrho \geq 0$ esetén $U\varrho U^* \geq 0$ és így $P \geq 0$ esetén $\operatorname{Tr}(\operatorname{Tr}_E U\varrho U^*)P = \operatorname{Tr}(U\varrho U^*)(P \otimes \mathrm{id}_E) > 0$. Mivel $T \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}(\varrho \otimes X) = \operatorname{Tr}_E(U \otimes \mathrm{id}_{\mathbb{C}^n})\varrho(U \otimes \mathrm{id}_{\mathbb{C}^n})^*$ is ilyen alakú, T teljesen pozitív.

$\operatorname{Tr}\operatorname{Tr}_E U\varrho U^* = \operatorname{Tr} U\varrho U^* = \operatorname{Tr} \varrho U^* U$ miatt a leképezés pontosan akkor trace-őrző, ha $U^*U = \mathrm{id}_{\mathcal{H}_A}$, vagyis ha U izometria.

A másik alaknál $\operatorname{Tr} \sum_{j=1}^r K_j \varrho K_j^* = \operatorname{Tr} \varrho \sum_{j=1}^r K_j^* K_j$, tehát a feltétel $\sum_{j=1}^r K_j^* K_j = \mathrm{id}_{\mathcal{H}_A}$. □

1.12. Definíció. Egy $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ lineáris leképezést (kvantum) csatornának nevezünk, ha teljesen pozitív és trace-őrző.

2. HF. Adjuk meg a $D_p : \mathcal{T}(\mathbb{C}^{\mathcal{X}}) \to \mathcal{T}(\mathbb{C}^{\mathcal{X}})$

$$D_p(\varrho) = (1-p)\varrho + p \sum_{x\in\mathcal{X}} \langle x|\varrho|x\rangle |x\rangle\langle x| \tag{1.10}$$

csatorna Kraus- és Stinespring-reprezentációját.

3. HF. Adjuk meg az $N_p : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H} \oplus \mathbb{C}^{\{e\}})$

$$N_p(\varrho) = (1-p)(\varrho \oplus 0) + p(0 \oplus |e\rangle\langle e|) \tag{1.11}$$

csatorna Kraus- és Stinespring-reprezentációját.

Megjegyzés. A $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ leképezés duálisa egy $T^* : \mathcal{B}(\mathcal{K}) \to \mathcal{B}(\mathcal{H})$ leképezés, ez pontosan akkor teljesen pozitív, ha T az. Továbbá T trace-őrző, ha T^* egységőrző.

1.13. Állítás. *Kvantum csatornák kompozíciója, tenzorszorzata kvantum csatorna.*

Bizonyítás. Ha $T_1 : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ és $T_2 : \mathcal{T}(\mathcal{K}) \to \mathcal{T}(\mathcal{L})$ teljesen pozitív leképezések, akkor $0 \le \varrho \in \mathcal{T}(\mathcal{H} \otimes \mathbb{C}^n)$ esetén

$$((T_2 \circ T_1) \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)})(\varrho) = ((T_2 \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}) \circ (T_1 \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}))(\varrho) \ge 0 \tag{1.12}$$

illetve $\mathrm{Tr}(T_2 \circ T_1)(\varrho) = \mathrm{Tr}(T_2(T_1(\varrho))) = \mathrm{Tr}(T_1(\varrho)) = 1$.

Legyenek $T_i : \mathcal{T}(\mathcal{H}_i) \to \mathcal{T}(\mathcal{K}_i)$ kvantum csatornák. Mivel $\mathrm{id}_{\mathcal{T}(\mathbb{C}^m)} \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)} = \mathrm{id}_{\mathcal{T}(\mathbb{C}^{mn})}$, ezért $T_1 \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_2)}$ és $\mathrm{id}_{\mathcal{T}(\mathcal{K}_1)} \otimes T_2$ is teljesen pozitív, kompozíciójuk pedig $T_1 \otimes T_2$. A trace-őrzést elég elemi tenzorokra belátni, ehhez elég meggondolni, hogy $\mathrm{Tr}(T_1 \otimes T_2)(\varrho \otimes \sigma) = \mathrm{Tr}\, T_1(\varrho)\, \mathrm{Tr}\, T_2(\sigma)$. □

1.14. Definíció. Legyenek $\mathcal{A}$ és $\mathcal{B}$ C*-algebrák. Egy $T : \mathcal{A} \to \mathcal{B}$ leképezés pozitív, ha $\forall A \in \mathcal{A} : T(A^*A) \ge 0$. T teljesen pozitív, ha $\forall n \in \mathbb{N} : T \otimes \mathrm{id}_{\mathcal{B}(\mathbb{C}^n)}$ pozitív. T egységőrző, ha $T(1_{\mathcal{A}}) = 1_{\mathcal{B}}$.

1.15. Állítás. *Legyenek $\mathcal{A}$ és $\mathcal{B}$ C*-algebrák, és tegyük fel, hogy az egyik kommutatív. Ekkor minden $T : A \to B$ pozitív leképezés teljesen pozitív.*

Bizonyítás. T pontosan akkor teljesen pozitív, ha T^* az, emiatt feltehető, hogy pl. $\mathcal{B}$ kommutatív. Legyen $\mathcal{B} \subseteq \mathcal{B}(\mathcal{H})$, $\psi_1, \ldots, \psi_n \in \mathcal{H}$ és $A_{ij} \in \mathcal{A}$ $(i, j = 1, 2, \ldots, n)$ olyan, hogy

$$\begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix} \ge 0 \tag{1.13}$$

Válasszunk egy olyan bázist $\mathcal{H}$-n, amiben $T(A_{ij})$ diagonális, ebben ψ_i komponenensei legyenek $\psi_{i,1}, \psi_{i,2}, \ldots$. Ekkor

$$\sum_{i,j=1}^{n} \langle \psi_i | T(A_{ij}) | \psi_j \rangle = \sum_{\beta} \langle \beta | \underbrace{T\left(\sum_{i,j=1}^{n} \overline{\psi_{i,\beta}} A_{ij} \psi_{j,\beta} \right)}_{\geq 0} | \beta \rangle \geq 0 \tag{1.14}$$

□

1.16. Következmény. *Legyen $\mathcal{H}$ Hilbert-tér, ekkor egy $T : \mathbb{C} \to \mathcal{T}(\mathcal{H})$ leképezés pontosan akkor teljesen pozitív, ha $T(1) \geq 0$. Eszerint $\mathcal{S}(\mathcal{H})^n$ ($\mathcal{S}_{\leq}(\mathcal{H})^n$) elemeit azonosíthatjuk a $T : \mathbb{C}^n \to \mathcal{T}(\mathcal{H})$ csatornák (teljesen pozitív nyomnemnövelő leképezések) terével.*

1.17. Állítás. *Legyenek $\mathcal{H}, \mathcal{K}$ véges dimenziós Hilbert-terek, $\mathcal{X}$ véges halmaz. Egy $T : \mathcal{T}(\mathcal{H}) \otimes \ell^1(\mathcal{X}) \to \mathcal{T}(\mathcal{K}) \otimes \ell^1(\mathcal{Y})$ lineáris leképezés pontosan akkor teljesen pozitív, ha*

$$T(\varrho \otimes |x\rangle\langle x|) = \sum_{i \in I_x} K_{x,i} \varrho K_{x,i}^* \otimes |f_x(i)\rangle\langle f_x(i)| \tag{1.15}$$

alakú, ahol I_x indexhalmaz, $K_{x,i} : \mathcal{H} \to \mathcal{K}$ lineáris leképezések, $f_x : I_x \to \mathcal{Y}$ függvény.

T pontosan akkor csatorna, ha a fenti felírásban $\sum_{i=1}^{r} K_{x,i}^* K_{x,i} = I$ minden $x \in \mathcal{X}$ esetén.

Bizonyítás. A fenti képlet által adott leképezés teljesen pozitív, mert

$$T(\cdot) = \sum_{\substack{x \in \mathcal{X} \\ i \in I_x}} \tilde{K}_{x,i} \cdot \tilde{K}_{x,i}^* \tag{1.16}$$

alakban is írható, ahol

$$\tilde{K}_{x,i} = (\mathrm{id}_{\mathcal{K}} \otimes |f_x(i)\rangle) K_{x,i} (\mathrm{id}_{\mathcal{H}} \otimes \langle x|) \tag{1.17}$$

Tegyük fel, hogy $T : \mathcal{T}(\mathcal{H}) \otimes \ell^1(\mathcal{X}) \to \mathcal{T}(\mathcal{K}) \otimes \ell^1(\mathcal{Y})$ teljesen pozitív, és legyen $\varrho_x : \mathcal{T}(\mathbb{C}) \to \ell^1(\mathcal{X})$ a $\varrho_x(1) = |x\rangle\langle x|$ módon adott leképezés, $D : \mathcal{T}(\mathbb{C}^{\mathcal{Y}}) \to \ell^1(\mathcal{Y})$, $D(\varrho) = \sum_{y \in \mathcal{Y}} \langle y|\varrho|y\rangle |y\rangle\langle y|$ és $E : \ell^1(\mathcal{Y}) \to \mathcal{T}(\mathbb{C}^{\mathcal{Y}})$ pedig a szokásos beágyazás. Ezekre $D \circ E = \mathrm{id}_{\ell^1(\mathcal{Y})}$ teljesül.

Mivel E és ϱ_x teljesen pozitív, $(\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes E) \circ T \circ (\mathrm{id}_{\mathcal{T}(\mathcal{H})} \otimes \varrho_x)$ is az, legyenek $\{M_{x,j}\}_{j \in J_x}$ a Kraus-operátorai. Ezzel

$$\begin{aligned} T(\varrho \otimes |x\rangle\langle x|) &= (\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes D) \circ (\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes E) \circ T \circ (\mathrm{id}_{\mathcal{T}(\mathcal{H})} \otimes \varrho_x)(\varrho) \\ &= \sum_{\substack{j \in J_x \\ y \in \mathcal{Y}}} (\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes |y\rangle\langle y|) M_{x,j} \varrho M_{x,j}^* (\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes |y\rangle\langle y|) \end{aligned} \tag{1.18}$$

ami éppen az állításban szereplő alakú, ha $I_x = J_x \times \mathcal{Y}$, $f_x((j,y)) = y$ és

$$K_{x,(j,y)} = (\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes \langle y|) M_{x,j} \tag{1.19}$$

□

1.18. Következmény. *Egy $M : \mathcal{T}(\mathcal{H}) \to \ell^1(\mathcal{Y})$ alakú csatorna egyértelműen megadható egy $E : \mathcal{Y} \to \mathcal{B}(\mathcal{H})$ POVM segítségével*

$$M(\varrho) = (\operatorname{Tr} \varrho E_y)_{y \in \mathcal{Y}} \tag{1.20}$$

módon.

Bizonyítás. Az előző állítást felhasználva léteznek olyan $K_i : \mathcal{H} \to \mathbb{C}$ szerint lineáris leképezések, amire

$$\begin{aligned} M(\varrho) &= \sum_{i \in I} K_i \varrho K_i^* |f(i)\rangle\langle f(i)| \\ &= \sum_{y \in \mathcal{Y}} \left(\sum_{i \in f^{-1}(y)} K_i \varrho K_i^* \right) |y\rangle\langle y| \\ &= \left(\operatorname{Tr} \varrho \sum_{i \in f^{-1}(y)} K_i^* K_i \right)_{y \in \mathcal{Y}} \end{aligned} \tag{1.21}$$

tehát léteznek egyértelmű E_y operátorok, amelyekkel M a fenti alakban írható. Mivel M pozitív, $E_y \geq 0$. $\operatorname{Tr}(\varrho) = \operatorname{Tr} M(\varrho)$ miatt $\sum_{y \in \mathcal{Y}} E_y = I$. □

Megjegyzés. Egy $M : \mathcal{T}(\mathcal{H}) \to \ell^1(\mathcal{Y})$ alakú csatornát mérésnek nevezünk.

1.19. Állítás. *Legyen $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna, és $U_i : \mathcal{H} \to \mathcal{K} \otimes \mathcal{H}_{E_i}$ olyanok, hogy $T(\varrho) = \operatorname{Tr}_{E_i} U_i \varrho U_i^*$ $(i = 1, 2)$. Ekkor létezik $V : \mathcal{H}_{E_1} \to \mathcal{H}_{E_2}$ parciális izometria, amivel $U_2 = (\mathrm{id}_{\mathcal{K}} \otimes V) \circ U_1$ teljesül. Ha $\dim \mathcal{H}_{E_1}$ minimális, akkor V egyértelmű és izometria.*

Bizonyítás. Legyen $\{|i\rangle\}_{i \in I}$ a $\mathcal{H}$ egy ortonormált bázisa, $|\Omega\rangle = \sum_{i \in I} |i\rangle \otimes |i\rangle \in \mathcal{H} \otimes \mathcal{H}$. Ha $\psi \in \mathcal{H} \otimes \mathcal{K}$, akkor

$$\begin{aligned} \langle\psi|(\mathrm{id}_{\mathcal{H}} \otimes T^*)(|\Omega\rangle\langle\Omega|)|\psi\rangle &= \langle\psi|(\mathrm{id}_{\mathcal{H}} \otimes U^*)(|\Omega\rangle\langle\Omega| \otimes \mathrm{id}_{\mathcal{H}_{E_i}})(\mathrm{id}_{\mathcal{H}} \otimes U)|\psi\rangle \\ &= \left\| (\langle\Omega| \otimes \mathrm{id}_{\mathcal{H}_{E_i}})(\mathrm{id}_{\mathcal{H}} \otimes U_i)|\psi\rangle \right\|^2 \end{aligned} \tag{1.22}$$

tehát ha $W_i = (\langle\Omega| \otimes \mathrm{id}_{\mathcal{H}_{E_i}}) \circ (\mathrm{id}_{\mathcal{H}} \otimes U_i)$, akkor $\|W_1|\psi\rangle\| = \|W_2|\psi\rangle\|$. Eszerint létezik olyan $V : \mathcal{H}_{E_1} \to \mathcal{H}_{E_2}$ parciális izometria, amire $W_2 = V \circ W_1$, és bármely két ilyen V megegyezik W_1 képterén.

Mivel $U \mapsto (\langle\Omega| \otimes \mathrm{id}_{\mathcal{H}_{E_i}}) \circ (\mathrm{id}_{\mathcal{H}} \otimes U)$ bijekció, ebből $U_2 = (\mathrm{id}_{\mathcal{K}} \otimes V) \circ U_1$ is következik. Ha $\dim \mathcal{H}_{E_1}$ minimális, akkor W_1 szürjektív, és így V egyértelmű. □

1.20. Definíció. Egy $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna kiterjesztése a $T' : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_E)$ csatorna, ha T előáll $T = (\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes \mathrm{Tr}_E) \circ T'$ módon.

Legyenek $T'_i : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_{E_i})$ a $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna kiterjesztései ($i = 1, 2$). Egy $\Phi : \mathcal{T}(\mathcal{H}_{E_1}) \to \mathcal{T}(\mathcal{H}_{E_2})$ csatorna ezen kiterjesztések közötti morfizmus, ha $T'_2 = (\mathrm{id}_{\mathcal{T}(\mathcal{K})} \otimes \Phi) \circ T'_1$.

Egy $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna univerzális kiterjesztése a $\tilde{T} : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_E)$ csatorna, ha kiterjesztés és minden $T' : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_{E'})$ kiterjesztéshez létezik egy Φ morfizmus $\tilde{T}$-ből T'-be.

1.21. Állítás. *Bármely $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatornának létezik univerzális kiterjesztése.*

Bizonyítás. Legyen $\tilde{T} : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_E)$, $\tilde{T}(\varrho) = U_1 \varrho U_1^*$ minimális Stinespring-reprezentáció. Ha $T' : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_{E'})$ is kiterjesztés, akkor létezik olyan további $T'' : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_{E'} \otimes \mathcal{H}_{E''})$, ami $T''(\varrho) = U_2 \varrho U_2^*$ alakú valamilyen U_2 izometriára.

A fenti állítás szerint létezik olyan $V : \mathcal{H}_E \to \mathcal{H}_{E'} \otimes \mathcal{H}_{E''}$ izometria, amire $U_2 = (\mathrm{id}_{\mathcal{K}} \otimes V) \circ U_1$. Ekkor $\Phi(\sigma) := \mathrm{Tr}_{E''} V \sigma V^*$ morfizmus $\tilde{T}$-ből T'-be.

□

Megjegyzés. Egy csatorna univerzális kiterjeszését izometrikus kiterjesztésnek nevezzük, egy állapot univerzális kiterjesztését pedig tiszta kiterjesztésnek (purification).

1.22. Definíció. Legyen a $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna izometrikus kiterjesztése $\tilde{T} : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K} \otimes \mathcal{H}_E)$. A $T^{\mathrm{c}} = \mathrm{Tr}_{\mathcal{K}} \circ \tilde{T}$ csatornát a T komplementerének (konjugáltjának) nevezzük.

A T csatorna degradálható, ha létezik olyan N csatorna, amire $T^{\mathrm{c}} = N \circ T$. T anti-degradálható, ha T^{c} degradálható.

Mivel $\tilde{T}$ a környezeten ható izometria erejégig egyértelmű, ezért T^{c} is az, illetve a degradálhatóság nem függ T^{c} választásától.

4. HF. Adjuk meg a $D_p : \mathcal{T}(\mathbb{C}^{\mathcal{X}}) \to \mathcal{T}(\mathbb{C}^{\mathcal{X}})$

$$D_p(\varrho) = (1-p)\varrho + p \sum_{x \in \mathcal{X}} \langle x|\varrho|x\rangle |x\rangle\langle x| \tag{1.23}$$

csatornának a komplementerét.

5. HF. Legyen $N_p : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H} \oplus \mathbb{C}^{\{e\}})$ az a csatorna, amire

$$N_p(\varrho) = (1-p)(\varrho \oplus 0) + p \operatorname{Tr} \varrho (0 \oplus |e\rangle\langle e|) \tag{1.24}$$

p milyen értékei mellett lesz ez degradálható illetve anti-degradálható?

1.23. Definíció. Legyenek $\mathcal{H}_A, \mathcal{H}_B$ Hilbert-terek. Egy $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ állapot szeparált, ha $\varrho_{i,A} \otimes \varrho_{i,B}$ alakú állapotok konvex kombinációjaként előáll. A nem szeparált állapotokat összefontnak nevezzük.

1.24. Példa.

$$\frac{1}{n} \sum_{i,i'=1}^{n} |i\rangle\langle i'| \otimes |i\rangle\langle i'| = \left(\frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle \right) \left(\frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle \right)^* \in \mathcal{S}(\mathbb{C}^n \otimes \mathbb{C}^n) \quad (1.25)$$

és lokális izometriákkal való konjugáltjainak neve (n szintű) teljesen összefont állapot.

1.25. Definíció. A T csatorna entanglement-breaking, ha minden $n \in \mathbb{N}$ esetén $T \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}$ bármely állapothoz szeparáltat rendel.

1.26. Állítás. *Legyen $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna. Ekkor a következők ekvivlensek:*

1. $$T(\varrho) = \sum_{i \in I} \varrho_i \operatorname{Tr}(\varrho E_i) \quad (1.26)$$
   ahol $E : I \to \mathcal{B}(\mathcal{H})$ POVM, $\varrho_i \in \mathcal{S}(\mathcal{K})$
2. *$T \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}(\varrho)$ minden n, ϱ esetén szeparált*
3. *$T \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}(|\Omega\rangle\langle\Omega|)$ szeparált, ahol $n = \dim \mathcal{H}$, $|\Omega\rangle\langle\Omega|$ teljesen összefont.*
4. *Létezik olyan $T(\varrho) = \sum_{i \in I} K_i B K_i^*$ Kraus-reprezentáció, amelyben* $\operatorname{rk} K_i = 1$

Bizonyítás. **1 $\Longrightarrow$ 2** Legyen $T_i(\varrho) = \varrho_i \operatorname{Tr}(\varrho E_i)$. Ekkor $(T_i \otimes \mathrm{id})(\sigma) = \operatorname{Tr}(\varrho E_i \otimes I)\varrho_i \otimes \operatorname{Tr}_{\mathcal{H}} \sigma$, tehát $(T \otimes \mathrm{id})(\sigma)$ szorzatállapotok konvex kombinációja.

2 $\Longrightarrow$ 3 Az utóbbi állítás az előbbi speciális esete.

3 $\Longrightarrow$ 4 Legyen

$$\begin{aligned} T \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}(|\Omega\rangle\langle\Omega|) &= \frac{1}{n} \sum_{i,j=1}^{n} T(|i\rangle\langle j|) \otimes |i\rangle\langle j| \\ &= \frac{1}{n} \sum_{k} \lambda_k p_k \otimes q_k \end{aligned} \quad (1.27)$$

ahol p_k, q_k egy rangú projekciók, $\lambda_k > 0$. Ha $p_k = |\eta_k\rangle\langle\eta_k|$ és $q_k = |\mu_k\rangle\langle\mu_k|$, akkor

$$T(|i\rangle\langle j|) = \sum_{k} \lambda_k \langle\eta_k|i\rangle\langle j|\eta_k\rangle |\mu_k\rangle\langle\mu_k| \quad (1.28)$$

tehát

$$T(\varrho) = \sum_{k} |\mu_k\rangle \sqrt{\lambda_k} \langle\eta_k|\varrho|\eta_k\rangle \sqrt{\lambda_k} \langle\mu_k| \quad (1.29)$$

4 $\implies$ 1 $|y\rangle\langle x|\varrho(|y\rangle\langle x|)^* = |y\rangle\langle y| \operatorname{Tr} \varrho|x\rangle\langle x|$ miatt igaz.

□

1.27. Példa. Legyen $\mathcal{H} = \mathcal{K} = \mathbb{C}^{\mathcal{X}}$. A

$$D(\varrho) := \sum_{x\in\mathcal{X}} \langle x|\varrho|x\rangle |x\rangle\langle x| \tag{1.30}$$

csatorna entanglement breaking (completely dephasing channel).

1.28. Példa. Legyenek $\mathcal{X}, \mathcal{Y}$ halmazok, $(S_{xy})_{x\in\mathcal{X},y\in\mathcal{Y}}$ sztochasztikus mátrix, azaz $S_{xy} \geq 0$ és $\sum_{y\in\mathcal{Y}} S_{xy} = 1$. Ekkor a $T_S : \mathcal{T}(\mathbb{C}^{\mathcal{X}}) \to \mathcal{T}(\mathbb{C}^{\mathcal{Y}})$

$$T(\varrho) = \sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} S_{xy} \langle x|\varrho|x\rangle |y\rangle\langle y| \tag{1.31}$$

csatorna entanglement breaking.

2. Távolságok

- állapotok, obszervábilisek vektorterekben vannak, távolságot definiálhatunk normák segítségével

2.1. Definíció. Egy $\|\cdot\| : \operatorname{Mat}(d,\mathbb{C}) \to \mathbb{R}_+$ függvény *unitér-invariáns norma*, ha norma (azaz $\|\alpha A\| = |A|\,\|A\|$, $\|A\| = 0 \implies A = 0$ és $\|A+B\| \leq \|A\| + \|B\|$) és bármely $A \in \operatorname{Mat}(d,\mathbb{C})$ és unitér U, V esetén $\|UAV\| = \|A\|$.

- tetszőleges $A \in \operatorname{Mat}(d,\mathbb{C})$ esetén létezik olyan U, V unitér mátrix, amire UAV diagonális nemnegatív elemekkel (szinguláris értékek), a főátló mentén csökkenő sorrendben
- unitér-invariáns norma csak a szinguláris értékektől függ
- pl. $\|A\|_1 = \operatorname{Tr}|A|$

2.2. Állítás. *Legyen $\|\cdot\|_{kl}$ olyan norma $\mathbb{R}^d$-en, ami csak a komponensek abszolútértékeitől függ és permutációinvariáns. Definiáljuk a $\|\cdot\| : \operatorname{Mat}(d,\mathbb{C}) \to \mathbb{R}_+$ függvényt olyan módon, hogy $\|A\|$ az A szinguláris értékeiből képzett $s(A)$ sorozat $\|s(A)\|_{kl}$ normája. Ekkor $\|\cdot\|$ unitér-invariáns norma.*

Bizonyítás. Bhatia - Matrix Analysis □

6. HF. Legyen $\|\cdot\|_{\mathrm{kl}} : \mathbb{R}^d \to \mathbb{R}_+$ olyan norma, ami csak a komponensek abszolútértékeitől függ és permutációinvariáns. Ekkor a

$$\|\omega\|'_{\mathrm{kl}} = \sup_{x:\|x\|_{\mathrm{kl}}\leq 1} |\omega(x)| \tag{2.1}$$

duális norma is permutációinvariáns és csak a komponensek abszolútértékétől függ. A $\|\cdot\|_{\mathrm{kl}}$ normából a fenti módon konstruált unitér-invariáns norma duálisa megegyezik a $\|\cdot\|'_{\mathrm{kl}}$ normából kapott unitér-invariáns normával.

2.3. Definíció. Az ℓ^p normákból a fenti módon konstruált unitér-invarins norma a Schatten-p-norma.

2.4. Példa. Legyen $\psi, \varphi \in \mathcal{H}$ két egységvektor. Ekkor $|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|$ önadjungált, 0 nyomú és rangja (legfeljebb) 2, tehát nullától különböző sajátértékei $\lambda, -\lambda$, ahol $0 \leq \lambda$ feltehető. Emiatt

$$\left\| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \right\|_p = (\lambda^p + \lambda^p)^{1/p} = 2^{1/p}\lambda \tag{2.2}$$

Speciálisan

$$\begin{aligned}
2\lambda^2 &= \left\| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \right\|_2^2 \\
&= \operatorname{Tr}(|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|)^2 \\
&= \operatorname{Tr}(|\psi\rangle\langle\psi| + |\varphi\rangle\langle\varphi| + |\psi\rangle\langle\psi,\varphi\rangle\langle\varphi| + |\varphi\rangle\langle\varphi,\psi\rangle\langle\psi|) \\
&= 2 + 2|\langle\psi,\varphi\rangle|^2
\end{aligned} \tag{2.3}$$

tehát

$$\left\| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \right\|_p = 2^{1/p}\sqrt{1 - |\langle\psi,\varphi\rangle|^2} \tag{2.4}$$

- a Schatten-normák tetszőleges $\mathcal{H}$ Hilbert-tér esetén értelmezhetőek $\mathcal{B}(\mathcal{H})$ azon elemeire, amelyek szinguláris értékeiből alkotott sorozatok abszolút értékeinek p-edik hatványa összegezhető
- adott p mellett ezek egy alteret alkotnak ($\mathcal{L}^p(\mathcal{H})$), ezeket az ℓ^p-terek nemkommutatív változatainak tekinthetjük, elemeik a Schatten-p-osztályú operátorok
- $p < \infty$ esetén a Schatten-p-osztályú operátorok kompaktak
- $p \leq p'$ esetén $\|\cdot\|_p \geq \|\cdot\|_{p'}$, tehát $\mathcal{L}^p(\mathcal{H}) \leq \mathcal{L}^{p'}(\mathcal{H})$

2.5. Állítás (Hölder-egyenlőtlenség)**.** *Legyen $\|\cdot\|$ unitér-invariáns norma. Ekkor $A, B \in \operatorname{Mat}(d, \mathbb{C})$ és $p^{-1} + q^{-1} = r^{-1}$ esetén*

$$\left\| |AB|^r \right\|^{1/r} \leq \left\| |A|^p \right\|^{1/p} \left\| |B|^q \right\|^{1/q} \tag{2.5}$$

teljesül.

Bizonyítás. Bhatia - Matrix Analysis □

2.6. Állítás. *Ha $A \in \mathcal{T}(\mathcal{H})$ és $B \in \mathcal{B}(\mathcal{H})$, akkor $|\operatorname{Tr} AB| \leq \|A\|_1 \|B\|_\infty$*

Bizonyítás. HF miatt elég: ℓ^1 és ℓ^∞ egymás duálisai véges dimenzióban. □

2.7. Állítás. *Legyen $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$. Ekkor*

$$\begin{aligned}
\frac{1}{2}\|\varrho - \sigma\|_1 &= \sup_{\substack{P \in \mathcal{B}(\mathcal{H}) \\ P = P^* = P^2}} |\operatorname{Tr} \varrho P - \operatorname{Tr} \sigma P| \\
&= \sup_{\substack{P \in \mathcal{B}(\mathcal{H}) \\ 0 \leq P \leq I}} |\operatorname{Tr} \varrho P - \operatorname{Tr} \sigma P|
\end{aligned} \tag{2.6}$$

Bizonyítás. Legyen $\varrho-\sigma$ pozitív része X, negatív része Y, azaz $\varrho-\sigma = X-Y$ és $|\varrho-\sigma| = X+Y$. Ekkor $\operatorname{Tr}(\varrho-\sigma)=0$ miatt $\operatorname{Tr} X = \operatorname{Tr} Y$, és így

$$\begin{aligned} |\operatorname{Tr} \varrho P - \operatorname{Tr} \sigma P| &= |\operatorname{Tr} XP - \operatorname{Tr} YP| \\ &\leq \max\{\operatorname{Tr} XP, \operatorname{Tr} YP\} \\ &\leq \max\{\operatorname{Tr} X, \operatorname{Tr} Y\} \\ &= \operatorname{Tr} X = \frac{1}{2}\|\varrho-\sigma\|_1 \end{aligned} \tag{2.7}$$

Ha P a $\operatorname{supp} X$ (vagy $\operatorname{supp} Y$) projektora, akkor itt egyenlőség van. □

2.8. Definíció. A $\varrho,\sigma \in \mathcal{S}(\mathcal{H})$ állapotok közötti fidelity

$$F(\varrho,\sigma) = \operatorname{Tr}\sqrt{\sqrt{\varrho}\sigma\sqrt{\varrho}} \tag{2.8}$$

(ennek a négyzetét is hívják fidelitynek...)

2.9. Definíció. A $\varrho,\sigma \in \mathcal{S}(\mathcal{H})$ állapotok közötti purified trace distance $P(\varrho,\sigma) = \sqrt{1-F(\varrho,\sigma)^2}$.

2.10. Példa. Legyen $\psi,\varphi \in \mathcal{H}$ két egységvektor. Ekkor

$$\begin{aligned} P(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|) &= \sqrt{1-F(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|)^2} \\ &= \sqrt{1-\left(\operatorname{Tr}\sqrt{\sqrt{|\psi\rangle\langle\psi|}|\varphi\rangle\langle\varphi|\sqrt{|\psi\rangle\langle\psi|}}\right)^2} \\ &= \sqrt{1-\left(\operatorname{Tr}\sqrt{|\psi\rangle\langle\psi||\varphi\rangle\langle\varphi||\psi\rangle\langle\psi|}\right)^2} \\ &= \sqrt{1-|\langle\psi,\varphi\rangle|^2} \\ &= \frac{1}{2}\||\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|\|_1 \end{aligned} \tag{2.9}$$

2.11. Tétel (Uhlmann). *Ha $\varrho,\sigma \in \mathcal{S}(\mathcal{H})$, akkor*

$$F(\varrho,\sigma) = \max_{\psi,\varphi} |\langle\psi,\varphi\rangle| \tag{2.10}$$

ahol ψ és φ a ϱ és σ tiszta kiterjesztésein fut végig.

Bizonyítás. Legyen $\{|i\rangle\}_{i\in I}$ a $\mathcal{H}$ egy ortonormált bázisa és

$$|\Omega\rangle = \sum_{i\in I} |i\rangle \otimes |i\rangle \in \mathcal{H}\otimes\mathcal{H} \tag{2.11}$$

Ekkor $|\psi\rangle = (\sqrt{\varrho} \otimes U)|\Omega\rangle$ és $|\varphi\rangle = (\sqrt{\sigma} \otimes V)|\Omega\rangle$ a ϱ és σ összes tiszta kiterjesztései, ahol U, V tetszőleges unitér operátorok. A kettő belső szorzata:

$$\begin{aligned}
\langle\psi,\varphi\rangle &= \langle\Omega, (\sqrt{\varrho}\otimes U^*)(\sqrt{\sigma}\otimes V)\Omega\rangle \\
&= \langle\Omega, (\sqrt{\varrho}\sqrt{\sigma}\otimes U^*V)\Omega\rangle \\
&= \sum_{i,i'}\langle i|\sqrt{\varrho}\sqrt{\sigma}|i'\rangle\langle i|U^*V|i'\rangle \\
&= \sum_{i,i'}\langle i|\sqrt{\varrho}\sqrt{\sigma}|i'\rangle\langle i'|(U^*V)^T|i\rangle \\
&= \operatorname{Tr}\sqrt{\varrho}\sqrt{\sigma}(U^*V)^T
\end{aligned} \tag{2.12}$$

Mivel $(U^*V)^T$ tetszőleges unitér operátor, a fenti belső szorzat abszolútértéke akkor maximális, ha $\sqrt{\varrho}\sqrt{\sigma}(U^*V)^T = |\sqrt{\varrho}\sqrt{\sigma}|$. □

2.12. Következmény. *Ha $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$, akkor*

$$P(\varrho,\sigma) = \min_{\psi,\varphi}\frac{1}{2}\,\||\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|\|_1 \tag{2.13}$$

2.13. Állítás. *Bármely $\varrho, \sigma, \varrho_i, \sigma_i \in \mathcal{S}(\mathcal{H})$, $U \in \mathcal{B}(\mathcal{H})$ unitér, $\alpha \in [0,1]$ esetén az alábbiak teljesülnek:*

1. $0 \leq F(\varrho,\sigma) \leq 1$
2. $F(\varrho,\sigma) = 1 \iff \varrho = \sigma$
3. $F(\varrho,\sigma) = 0 \iff \operatorname{supp}\varrho \perp \operatorname{supp}\sigma$
4. $F(\varrho,\sigma) = F(\sigma,\varrho)$
5. $F(\varrho_1\otimes\varrho_2, \sigma_1\otimes\sigma_2) = F(\varrho_1,\sigma_1)F(\varrho_2,\sigma_2)$
6. $F(U\varrho U^*, U\sigma U^*) = F(\varrho,\sigma)$
7. $$F(\sum_{x\in\mathcal{X}} P_X(x)\varrho_x, \sum_{x\in\mathcal{X}} P_X(x)\sigma_x)^2 \geq \sum_{x\in\mathcal{X}} P_X(x)F(\varrho_x,\sigma_x)^2 \tag{2.14}$$

Bizonyítás. **1** $0 \leq |\langle\psi,\varphi\rangle| \leq$.

2 Ha $\varrho = \sigma$, akkor $\|\sqrt{\varrho}\sqrt{\sigma}\|_1 = \|\varrho\|_1 = 1$. Ha $F(\varrho,\sigma) = 1$, akkor létezik olyan tiszta kiterjesztésük, amik megegyeznek, ekkor viszont ezek redukált állapota is megegyezik.

3 $F(\varrho,\sigma) = \|\sqrt{\varrho}\sqrt{\sigma}\|_1 = 0 \iff \sqrt{\varrho}\sqrt{\sigma} = 0 \iff \operatorname{supp}\sqrt{\varrho} \perp \operatorname{supp}\sqrt{\sigma} \iff \operatorname{supp}\varrho \perp \operatorname{supp}\sigma$

4 $F(\varrho,\sigma) = \|\sqrt{\varrho}\sqrt{\sigma}\|_1 = \|(\sqrt{\varrho}\sqrt{\sigma})^*\|_1 = \|\sqrt{\sigma}\sqrt{\varrho}\|_1 = F(\sigma,\varrho)$

5

$$\begin{aligned}
&F(\varrho_1 \otimes \varrho_2, \sigma_1 \otimes \sigma_2) \\
&= \operatorname{Tr} \sqrt{\sqrt{\varrho_1 \otimes \varrho_2}(\sigma_1 \otimes \sigma_2)\sqrt{\varrho_1 \otimes \varrho_2}} \\
&= \operatorname{Tr} \sqrt{(\sqrt{\varrho_1} \otimes \sqrt{\varrho_2})(\sigma_1 \otimes \sigma_2)(\sqrt{\varrho_1} \otimes \sqrt{\varrho_2})} \\
&= \operatorname{Tr} \sqrt{(\sqrt{\varrho_1}\sigma_1\sqrt{\varrho_1}) \otimes (\sqrt{\varrho_2}\sigma_2\sqrt{\varrho_2})} \\
&= \operatorname{Tr} \sqrt{\sqrt{\varrho_1}\sigma_1\sqrt{\varrho_1}} \otimes \sqrt{\sqrt{\varrho_2}\sigma_2\sqrt{\varrho_2}} \\
&= F(\varrho_1, \sigma_1)F(\varrho_2, \sigma_2)
\end{aligned} \tag{2.15}$$

6

$$\begin{aligned}
F(U\varrho U^*, U\sigma U^*) &= \operatorname{Tr} \sqrt{\sqrt{U\varrho U^*}U\sigma U^*\sqrt{U\varrho U^*}} \\
&= \operatorname{Tr} \sqrt{U\sqrt{\varrho}U^*U\sigma U^*U\sqrt{\varrho}U^*} \\
&= \operatorname{Tr} U\sqrt{\sqrt{\varrho}\sigma\sqrt{\varrho}}U^* \\
&= \operatorname{Tr} \sqrt{\varrho\sigma\sqrt{\varrho}} = F(\varrho, \sigma)
\end{aligned} \tag{2.16}$$

7 Legyenek $|\phi_{\varrho_x}\rangle, |\phi_{\sigma_x}\rangle$ olyan tiszta kiterjesztések, amelyekre $F(\varrho_x, \sigma_x) = |\langle\phi_{\varrho_x}, \sigma_{\varrho_x}\rangle|$ és legyen

$$|\phi_\varrho\rangle = \sum_{x\in\mathcal{X}} \sqrt{P_X(x)}|\phi_{\varrho_x}\rangle \otimes |x\rangle \tag{2.17}$$

$$|\phi_\sigma\rangle = \sum_{x\in\mathcal{X}} \sqrt{P_X(x)}|\phi_{\sigma_x}\rangle \otimes |x\rangle \tag{2.18}$$

Ekkor

$$\begin{aligned}
F\left(\sum_{x\in\mathcal{X}} P_X(x)\varrho_x, \sum_{x\in\mathcal{X}} P_X(x)\sigma_x\right)^2 &\geq |\langle\phi_\varrho, \phi_\sigma\rangle|^2 \\
&= \sum_{x\in\mathcal{X}} P_X(x)|\langle\phi_{\varrho_x}, \phi_{\sigma_x}\rangle|^2 \\
&= \sum_{x\in\mathcal{X}} P_X(x)F(\varrho_x, \sigma_x)^2
\end{aligned} \tag{2.19}$$

□

7. HF. $\mathcal{T}(\mathbb{C}^2)$ egy bázisa

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.20}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.21}$$

Minden állapot felírható

$$\frac{1}{2}(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z) \equiv \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}) \tag{2.22}$$

alakban, ahol $\|\vec{r}\|^2 = r_x^2 + r_y^2 + r_z^2 \leq 1$.

Legyen $\varrho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})$ és $\sigma = \frac{1}{2}(I + \vec{s}\cdot\vec{\sigma})$. Számoljuk ki $\|\varrho - \sigma\|_1$ és $F(\varrho, \sigma)$ értékét.

2.14. Állítás. *Legyen $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$, $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna. Ekkor*

1. $\|T(\varrho) - T(\sigma)\|_1 \leq \|\varrho - \sigma\|_1$
2. $F(T(\varrho), T(\sigma)) \geq F(\varrho, \sigma)$
3. $P(T(\varrho), T(\sigma)) \leq P(\varrho, \sigma)$

1 akkor is igaz, ha T pozitív és trace-őrző.

Bizonyítás. **1** Legyen $0 \leq P \leq I$ olyan, hogy $\frac{1}{2}\|T(\varrho) - T(\sigma)\|_1 = |\operatorname{Tr} T(\varrho)P - \operatorname{Tr} T(\sigma)P)|$. Ekkor $0 \leq T^*(P) \leq I$ és így

$$\begin{aligned} \|\varrho - \sigma\|_1 &\geq |\operatorname{Tr} \varrho T^*(P) - \operatorname{Tr} \sigma T^*(P)| \\ &= |\operatorname{Tr} T(\varrho)P - \operatorname{Tr} T(\sigma)P)| \\ &= \|T(\varrho) - T(\sigma)\|_1 \end{aligned} \tag{2.23}$$

2 Minden csatorna felírható $T(\varrho) = \operatorname{Tr}_E U\varrho U^*$ alakban. Láttuk, hogy $F(U\varrho U^*, U\sigma U^*) = F(\varrho, \sigma)$, így elég azt megmutatni, hogy $F(\operatorname{Tr}_E \varrho, \operatorname{Tr}_E \sigma) \geq F(\varrho, \sigma)$. Legyen $|\psi\rangle\langle\psi|$ és $|\varphi\rangle\langle\varphi|$ a ϱ és a σ tiszta kiterjesztései, amelyekre $F(\varrho, \sigma) = F(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|)$. Ezek $\operatorname{Tr}_E \varrho$, $\operatorname{Tr}_E \sigma$-nak is tiszta kiterjesztései, így

$$\begin{aligned} F(\operatorname{Tr}_E \varrho, \operatorname{Tr}_E \sigma) &\geq F(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|) \\ &= F(\varrho, \sigma) \end{aligned} \tag{2.24}$$

3

$$\begin{aligned} P(T(\varrho), T(\sigma)) &= \sqrt{1 - F(T(\varrho), T(\sigma))^2} \\ &\leq \sqrt{1 - F(\varrho, \sigma)^2} \\ &= P(\varrho, \sigma) \end{aligned} \tag{2.25}$$

□

2.15. Állítás (Fidelity és trace distance ekvivalenciája)**.**

$$1 - F(\varrho, \sigma) \leq \frac{1}{2}\|\varrho - \sigma\|_1 \leq \sqrt{1 - F(\varrho, \sigma)^2} \tag{2.26}$$

Bizonyítás. Láttuk, hogy $\sqrt{1 - F(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|)^2} = \frac{1}{2} \left\| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \right\|_1$. Legyen most ϱ, σ tetszőleges, $|\psi\rangle\langle\psi|$, $|\varphi\rangle\langle\varphi|$ pedig olyan tiszta kiterjesztések, amelyekre $F(\varrho, \sigma) = F(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|)$. Ekkor

$$\begin{aligned} \frac{1}{2} \left\| \varrho - \sigma \right\|_1 &\leq \frac{1}{2} \left\| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \right\| \\ &= \sqrt{1 - F(|\psi\rangle\langle\psi|, |\varphi\rangle\langle\varphi|)^2} \\ &= \sqrt{1 - F(\varrho, \sigma)^2} \end{aligned} \tag{2.27}$$

A másik irányhoz tekintsük a $\operatorname{Tr}(\sqrt{\varrho} - \sqrt{\sigma})^2$ mennyiséget. Erre

$$\begin{aligned} \operatorname{Tr}(\sqrt{\varrho} - \sqrt{\sigma})^2 &= \operatorname{Tr}(\varrho + \sigma - \sqrt{\varrho}\sqrt{\sigma} - \sqrt{\sigma}\sqrt{\varrho}) \\ &= 2 - 2 \operatorname{Tr} \sqrt{\varrho}\sqrt{\sigma} \\ &\geq 2 - 2 \operatorname{Tr} |\sqrt{\varrho}\sqrt{\sigma}| \\ &= 2 - 2F(\varrho, \sigma) \end{aligned} \tag{2.28}$$

teljesül. Legyen U olyan unitér operátor, amire $U(\sqrt{\varrho} - \sqrt{\sigma}) = (\sqrt{\varrho} - \sqrt{\sigma})U = |\sqrt{\varrho} - \sqrt{\sigma}|$, ilyen létezik, mert $\sqrt{\varrho} - \sqrt{\sigma}$ önadjungált. Legyen $|\sqrt{\varrho} - \sqrt{\sigma}| = \sum_{i \in I} \lambda_i |\psi_i\rangle\langle\psi_i|$, ahol $\| |\psi_i\rangle \| = 1$. Ekkor

$$\begin{aligned} \left\| \varrho - \sigma \right\|_1 &= \operatorname{Tr} |\varrho - \sigma| \\ &\geq |\operatorname{Tr}(\varrho - \sigma)U| \\ &= |\operatorname{Tr}(\frac{1}{2}(\sqrt{\varrho} - \sqrt{\sigma})(\sqrt{\varrho} + \sqrt{\sigma}) + \frac{1}{2}(\sqrt{\varrho} + \sqrt{\sigma})(\sqrt{\varrho} - \sqrt{\sigma}))U| \\ &= \operatorname{Tr}(|\sqrt{\varrho} - \sqrt{\sigma}|(\sqrt{\varrho} + \sqrt{\sigma})) \\ &= \sum_{i \in I} |\lambda_i| \langle\psi_i|(\sqrt{\varrho} + \sqrt{\sigma})|\psi_i\rangle \\ &\geq \sum_{i \in I} |\lambda_i| \left| \langle\psi_i|(\sqrt{\varrho}|\psi_i\rangle - \langle\psi_i|\sqrt{\sigma})|\psi_i\rangle \right| \\ &= \sum_{i \in I} |\lambda_i|^2 = \operatorname{Tr}(\sqrt{\varrho} - \sqrt{\sigma})^2 \end{aligned} \tag{2.29}$$

□

2.16. Állítás (Gentle measurement (gyengéd, enyhe, szelíd, finom, udvarias, tapintatos?))**.** *Legyen* $\varrho \in \mathcal{S}(\mathcal{H})$ *és* $\Lambda \in \mathcal{B}(\mathcal{H})$*,* $0 \leq \Lambda \leq I$*. Tegyük fel, hogy* $\operatorname{Tr} \varrho\Lambda \geq 1 - \varepsilon$*. Ekkor*

$$\frac{1}{2} \left\| \varrho \otimes |0\rangle\langle 0| - (\sqrt{\Lambda}\varrho\sqrt{\Lambda} \otimes |0\rangle\langle 0| + \sqrt{I - \Lambda}\varrho\sqrt{I - \Lambda} \otimes |1\rangle\langle 1|) \right\|_1 \leq 2\sqrt{\varepsilon} \tag{2.30}$$

Bizonyítás. Feltehető, hogy ϱ tiszta, mert ha $\varrho = \operatorname{Tr}_E |\varphi\rangle\langle\varphi|$, akkor $\operatorname{Tr} |\varphi\rangle\langle\varphi|(\Lambda \otimes I_E) = \operatorname{Tr} \varrho\Lambda$ és

$$\begin{aligned}
&\left\| \varrho \otimes |0\rangle\langle 0| - (\sqrt{\Lambda}\varrho\sqrt{\Lambda} \otimes |0\rangle\langle 0| + \sqrt{I-\Lambda}\varrho\sqrt{I-\Lambda} \otimes |1\rangle\langle 1|) \right\|_1 \\
\leq &\left\| |\varphi\rangle\langle\varphi| \otimes |0\rangle\langle 0| - (\sqrt{\Lambda \otimes I_E}|\varphi\rangle\langle\varphi|\sqrt{\Lambda \otimes I_E} \otimes |0\rangle\langle 0| + \sqrt{I \otimes I_E - \Lambda \otimes I_E}\varrho\sqrt{I \otimes I_E - \Lambda \otimes I_E} \otimes |1\rangle \right.
\end{aligned} \tag{2.31}$$

Ha $\varrho = |\varphi\rangle\langle\varphi|$, akkor viszont

$$\begin{aligned}
F\left(|\varphi\rangle\langle\varphi|, \frac{\sqrt{\Lambda}\varrho\sqrt{\Lambda}}{\operatorname{Tr} |\varphi\rangle\langle\varphi|\Lambda}\right)^2 &= |\langle\varphi|\frac{\sqrt{\Lambda}\varrho\sqrt{\Lambda}}{\operatorname{Tr} |\varphi\rangle\langle\varphi|\Lambda}|\varphi\rangle| \\
&= \frac{\langle\varphi|\sqrt{\Lambda}|\varphi\rangle^2}{\operatorname{Tr} |\varphi\rangle\langle\varphi|\Lambda} \\
&\geq \frac{\langle\varphi|\Lambda|\varphi\rangle^2}{\operatorname{Tr} |\varphi\rangle\langle\varphi|\Lambda} \\
&= \operatorname{Tr} |\varphi\rangle\langle\varphi|\Lambda
\end{aligned} \tag{2.32}$$

és így

$$\begin{aligned}
&\frac{1}{2}\left\| \varrho \otimes |0\rangle\langle 0| - (\sqrt{\Lambda}\varrho\sqrt{\Lambda} \otimes |0\rangle\langle 0| + \sqrt{I-\Lambda}\varrho\sqrt{I-\Lambda} \otimes |1\rangle\langle 1|) \right\|_1 \\
&\leq \sqrt{1 - F(\varrho \otimes |0\rangle\langle 0|, (\sqrt{\Lambda}\varrho\sqrt{\Lambda} \otimes |0\rangle\langle 0| + \sqrt{I-\Lambda}\varrho\sqrt{I-\Lambda} \otimes |1\rangle\langle 1|))^2} \\
&\leq \sqrt{1 - (Tr\varrho\Lambda)F\left(\varrho, \frac{\sqrt{\Lambda}\varrho\sqrt{\Lambda}}{\operatorname{Tr} \varrho\Lambda}\right)^2} \\
&\leq \sqrt{1 - (Tr\varrho\Lambda)^2} \\
&\leq 2\sqrt{\varepsilon}
\end{aligned} \tag{2.33}$$

□

2.17. Definíció. Legyen $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna. Ekkor

$$\eta[T] := \sup_{\substack{\varrho,\sigma \in \mathcal{S}(\mathcal{H}) \\ \varrho \neq \sigma}} \frac{\|T(\varrho) - T(\sigma)\|_1}{\|\varrho - \sigma\|_1} \tag{2.34}$$

a csatorna trace-távolság kontrakciós együtthatója.

8. HF. Bármely $T : \mathcal{T}(\mathbb{C}^2) \to \mathcal{T}(\mathbb{C}^2)$ csatorna mátrixa az $I, \sigma_x, \sigma_y, \sigma_z$ bázisban kifejtve

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ t_x & a_{xx} & a_{xy} & a_{xz} \\ t_y & a_{yx} & a_{yy} & a_{yz} \\ t_z & a_{zx} & a_{zy} & a_{zz} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \vec{t} & A \end{pmatrix} \tag{2.35}$$

alakú. Mennyi ennek a trace-távolság kontrakciós együtthatója?

Ha $T(\varrho) = U\varrho U^* =: \Gamma_U(\varrho)$ valamely U unitér operátorral, akkor $\vec{t} = 0$ és $A \in \mathrm{SO}(3)$, így mindig lehet találni olyan U, V unitéreket, amivel $\Gamma_U \circ T \circ \Gamma_V$ mátrixában a jobb alsó elem diagonális. Hogyan lehet ezen diagonális elemekkel kifejezni a trace-távolság kontrakciós együtthatót?

2.18. Állítás. *Legyenek $T_1 : \mathcal{T}(\mathcal{H}_1) \to \mathcal{T}(\mathcal{H}_2)$ és $T_2 : \mathcal{T}(\mathcal{H}_2) \to \mathcal{T}(\mathcal{H}_3)$ csatornák. Ekkor $\eta[T_2 \circ T_1] \leq \eta[T_1]\eta[T_2]$.*

Bizonyítás.

$$\begin{aligned} &\frac{\|(T_2 \circ T_1)(\varrho) - (T_2 \circ T_1)(\sigma)\|_1}{\|\varrho - \sigma\|_1} \\ &\qquad = \frac{\|(T_2 \circ T_1)(\varrho) - (T_2 \circ T_1)(\sigma)\|_1}{\|T_1(\varrho) - T_1(\sigma)\|_1} \frac{\|T_1(\varrho) - T_1(\sigma)\|_1}{\|\varrho - \sigma\|_1} \\ &\qquad\qquad \leq \eta[T_1]\eta[T_2] \end{aligned} \tag{2.36}$$

A bal oldal szuprémuma $\eta[T_2 \circ T_1]$, így ez is kisebb a jobb oldalnál. □

2.19. Állítás. *Legyen $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ kvantum csatorna. Ekkor*

$$\eta[T] = \frac{1}{2} \sup_{\psi \perp \varphi} \|T(|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|)\|_1 \tag{2.37}$$

Bizonyítás. $\||\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|\|_1 = 2$ miatt a jobb oldal alsó korlát, mivel kisebb halmazon tekintjük ugyanannak a kifejezésnek a szuprémumát.

Ha $\eta[T] = \|T(\varrho - \sigma)\|_1 / \|\varrho - \sigma\|_1$ és $P_\pm$ a $\varrho - \sigma$ pozitív és negatív része, akkor

$$\frac{\left\|T\left(\frac{P_+}{\operatorname{Tr} P_+}\right) - T\left(\frac{P_-}{\operatorname{Tr} P_+}\right)\right\|_1}{\left\|\left(\frac{P_+}{\operatorname{Tr} P_+}\right) - \left(\frac{P_-}{\operatorname{Tr} P_+}\right)\right\|_1} \tag{2.38}$$

tehát feltehető, hogy ϱ és σ ortogonálisak, ekkor $\|\varrho - \sigma\|_1 = 2$. Legyen $\varrho = \sum_{i \in I} \lambda_i |\psi_i\rangle\langle\psi_i|$ és $\sigma = \sum_{i \in I} \lambda_i |\varphi_i\rangle\langle\varphi_i|$ konvex dekompozíció, ekkor

$$\begin{aligned} \|T(\varrho - \sigma)\|_1 &= \left\| \sum_{i \in I} \lambda_i T(|\psi_i\rangle\langle\psi_i| - |\varphi_i\rangle\langle\varphi_i|) \right\|_1 \\ &\leq \sum_{i \in I} \lambda_i \|T(|\psi_i\rangle\langle\psi_i| - |\varphi_i\rangle\langle\varphi_i|)\|_1 \end{aligned} \tag{2.39}$$

tehát a jobb oldalon van olyan i, hogy $\||\psi_i\rangle\langle\psi_i| - |\varphi_i\rangle\langle\varphi_i|\|_1 = \eta[T]$. □

2.20. Tétel (Kvantum Döblin-tétel)**.** *Legyenek $T, T' : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ trace- és *-őrző lineáris leképezések, $T'(\varrho) = \tau \operatorname{Tr} \varrho$, $\varepsilon > 0$. Ha $T - \varepsilon T'$ pozitív leképezés, akkor $\eta[T] \leq 1 - \varepsilon$.*

Bizonyítás. Ha $\varrho_1, \varrho_2 \in \mathcal{S}(\mathcal{H})$, akkor

$$\begin{aligned}
\left\|T(\varrho_1) - T(\varrho_2)\right\|_1 &= \left\|T(\varrho_1) - \varepsilon T'(\varrho_1) - T(\varrho_2) + \varepsilon T'(\varrho_2)\right\|_1 \\
&= (1-\varepsilon)\left\|\frac{T-\varepsilon T'}{1-\varepsilon}(\varrho_1) - \frac{T-\varepsilon T'}{1-\varepsilon}(\varrho_2)\right\|_1 \\
&\leq (1-\varepsilon)\left\|\varrho_1 - \varrho_2\right\|_1
\end{aligned} \tag{2.40}$$

□

2.21. Definíció. Egy $\Phi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ lineáris leképezés $1-1$-normája

$$\left\|\Phi\right\|_{1-1} = \sup_{X:\left\|X\right\|_1 \leq 1} \left\|\Phi(X)\right\|_1 \tag{2.41}$$

- ha T csatorna, akkor $\left\|T\right\|_{1-1} = 1$
- kompozícióra szubmultiplikatív, mert indukált operátornorma
- $\left\|T - T'\right\|_{1-1}$ két csatorna különbözőségét méri: ha ugyanaz az állapot a két csatorna bemenete, a kimeneteken ugyanazt a mérést végezzük el, ez a maximális valószínűsége annak, hogy meg tudjuk őket különböztetni
- ha megengedjük, hogy egy összetett rendszer részén hasson a csatorna, akkor ez már nem igaz

2.22. Állítás. *Legyenek $T_1, T_1' : \mathcal{T}(\mathcal{H}_1) \to \mathcal{T}(\mathcal{H}_2)$ és $T_2, T_2' : \mathcal{T}(\mathcal{H}_2) \to \mathcal{T}(\mathcal{H}_3)$ csatornák. Ekkor*

$$\left\|T_2 \circ T_1 - T_2' \circ T_1'\right\|_{1-1} \leq \left\|T_1 - T_1'\right\|_{1-1} + \left\|T_2 - T_2'\right\|_{1-1} \tag{2.42}$$

Bizonyítás.

$$\begin{aligned}
\left\|T_2 \circ T_1 - T_2' \circ T_1'\right\|_{1-1} &= \left\|T_2 \circ T_1 - T_2' \circ T_1 + T_2' \circ T_1 - T_2' \circ T_1'\right\|_{1-1} \\
&\leq \left\|T_2 \circ T_1 - T_2' \circ T_1\right\|_{1-1} + \left\|T_2' \circ T_1 - T_2' \circ T_1'\right\|_{1-1} \\
&\leq \left\|T_2 - T_2'\right\|_{1-1} \left\|T_1\right\|_{1-1} + \left\|T_2'\right\|_{1-1} \left\|T_1 - T_1'\right\|_{1-1} \\
&= \left\|T_1 - T_1'\right\|_{1-1} + \left\|T_2 - T_2'\right\|_{1-1}
\end{aligned} \tag{2.43}$$

□

9. HF. Egy $T : \mathcal{T}(\mathbb{C}^2) \to \mathcal{T}(\mathbb{C}^2)$ csatorna mátrixa az $I, \sigma_x, \sigma_y, \sigma_z$ bázisban

$$\begin{pmatrix} 1 & 0 \\ \vec{t} & A \end{pmatrix} \tag{2.44}$$

Mennyi a $\left\|T - \mathrm{id}_{\mathcal{T}(\mathbb{C}^2)}\right\|_{1-1}$ távolság?

2.23. Definíció. Egy $\Phi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ lineáris leképezés diamond-normája (káró-norma?)

$$\|\Phi\|_\Diamond = \sup_{n \in \mathbb{N}} \left\| \Phi \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)} \right\|_{1-1} \tag{2.45}$$

- ha T csatorna, akkor $\|T\|_\Diamond = 1$
- $\|T - T'\|_{1-1}$ és $\|T - T'\|_\Diamond$ nagyon különbözhetnek

2.24. Példa. Legyen $T_+, T_- : \mathcal{T}(\mathbb{C}^n) \to \mathcal{T}(\mathbb{C}^n)$

$$T_\pm(\varrho) = \frac{(\mathrm{Tr}\,\varrho)I \pm \varrho^T}{n \pm 1} \tag{2.46}$$

Mindkettő teljesen pozitív és trace-őrző. Ha $\|X\|_1 \leq 1$, akkor

$$\begin{aligned} \|T_+(X) - T_-(X)\|_1 &= 2 \left\| \frac{(\mathrm{Tr}\,X)I - nX^T}{n^2 - 1} \right\|_1 \\ &\leq 2 \left\| \frac{(\mathrm{Tr}\,X)I}{n^2-1} \right\|_1 + 2 \left\| \frac{nX^T}{n^2-1} \right\|_1 \\ &\leq \frac{4n}{n^2-1} \end{aligned} \tag{2.47}$$

Másrészt ha

$$|\Omega\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle \otimes |i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n \tag{2.48}$$

akkor

$$\begin{aligned} \|T_+ - T_-\|_\Diamond &\geq \left\| T_+ \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)} - T_- \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)} \right\|_{1-1} \\ &\geq \left\| T_+ \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}(|\Omega\rangle\langle\Omega|) - T_- \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^n)}(|\Omega\rangle\langle\Omega|) \right\|_1 \\ &= \frac{2}{n^2-1} \left\| I \otimes \frac{I}{n} - \sum_{i,i'=1}^n |i'\rangle\langle i| \otimes |i\rangle\langle i'| \right\|_1 \\ &= 2\frac{n^2-1}{n^2-1} \end{aligned} \tag{2.49}$$

mert $\sum_{i,i'=1}^n |i'\rangle\langle i| \otimes |i\rangle\langle i'|$ önadjungált, négyzete az identitás, így két ortogonális projektor különbsége, a dimenziók összege n^2, különbsége n. Eszerint $\frac{n^2 \pm n}{2}$ dimenziósak, a különbségnek kétféle sajátértéke van, $1 + \frac{1}{n}$ multiplicitása $\frac{n^2-n}{2}$, míg $-1 + \frac{1}{n}$ multiplicitása $\frac{n^2+n}{2}$. Tehát

$$\begin{aligned} &\left\| I \otimes \frac{I}{n} - \sum_{i,i'=1}^n |i'\rangle\langle i| \otimes |i\rangle\langle i'| \right\|_1 \\ &\qquad = \frac{n^2-n}{2}\left(1 + \frac{1}{n}\right) + \frac{n^2+n}{2}\left(1 - \frac{1}{n}\right) = n^2 - 1 \end{aligned} \tag{2.50}$$

2.25. Állítás. *Legyenek $T_1, T_1' : \mathcal{T}(\mathcal{H}_1) \to \mathcal{T}(\mathcal{H}_2)$ és $T_2, T_2' : \mathcal{T}(\mathcal{H}_2) \to \mathcal{T}(\mathcal{H}_3)$ csatornák. Ekkor*

$$\left\|T_2 \circ T_1 - T_2' \circ T_1'\right\|_\Diamond \le \left\|T_1 - T_1'\right\|_\Diamond + \left\|T_2 - T_2'\right\|_\Diamond \tag{2.51}$$

Bizonyítás.

$$\begin{aligned} \left\|T_2 \circ T_1 - T_2' \circ T_1'\right\|_\Diamond &= \left\|T_2 \circ T_1 - T_2' \circ T_1 + T_2' \circ T_1 - T_2' \circ T_1'\right\|_\Diamond \\ &\le \left\|T_2 \circ T_1 - T_2' \circ T_1\right\|_\Diamond + \left\|T_2' \circ T_1 - T_2' \circ T_1'\right\|_\Diamond \\ &\le \left\|T_2 - T_2'\right\|_\Diamond \left\|T_1\right\|_\Diamond + \left\|T_2'\right\|_\Diamond \left\|T_1 - T_1'\right\|_\Diamond \\ &= \left\|T_1 - T_1'\right\|_\Diamond + \left\|T_2 - T_2'\right\|_\Diamond \end{aligned} \tag{2.52}$$

□

10. HF. Legyen $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ lineáris leképezés és $\mathcal{H}'$ Hilbert-tér. Ekkor

$$\left\|T \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}')}\right\|_\Diamond = \|T\|_\Diamond \tag{2.53}$$

2.26. Következmény. *Legyenek $T_i, T_i' : \mathcal{T}(\mathcal{H}_i) \to \mathcal{T}(\mathcal{K}_i)$ csatornák ($i = 1, 2$). Ekkor*

$$\left\|T_1 \otimes T_2 - T_1' \otimes T_2'\right\|_\Diamond \le \left\|T_1 - T_1'\right\|_\Diamond + \left\|T_2 - T_2'\right\|_\Diamond \tag{2.54}$$

Bizonyítás.

$$\begin{aligned} \left\|T_1 \otimes T_2 - T_1' \otimes T_2'\right\|_\Diamond &= \left\|(T_1 \otimes \mathrm{id}) \circ (\mathrm{id} \otimes T_2) - (T_1' \otimes \mathrm{id}) \circ (\mathrm{id} \otimes T_2')\right\|_\Diamond \\ &\le \left\|T_1 \otimes \mathrm{id} - T_1' \otimes \mathrm{id}\right\|_\Diamond + \left\|\mathrm{id} \otimes T_2 - \mathrm{id} \otimes T_2'\right\|_\Diamond \\ &= \left\|T_1 - T_1'\right\|_\Diamond + \left\|T_2 - T_2'\right\|_\Diamond \end{aligned} \tag{2.55}$$

□

3. Spektrális tulajdonságok

- egy $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ csatorna lineáris transzformáció, tehát vannak sajátértékei, sajátvektorai, determinánsa
- érdekes lehet pl. $T^n(\varrho)$ állapotsorozat vizsgálatánál

3.1. Állítás. *Ha $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ önadjungált operátorokat önadjungáltba visz, akkor ha λ sajátértéke, akkor $\overline{\lambda}$ is az.*

Ha $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ pozitív leképezés, akkor $\varrho(T) \le \|T^*(I)\|_\infty$. Ha T nyomőrző, akkor az 1 sajátértéke és $\varrho(T) = 1$.

Ha $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ csatorna, λ sajátértéke és $|\lambda| = 1$, akkor λ geometriai és algebrai multiplicitása megegyezik.

Bizonyítás. Minden $X \in \mathcal{T}(\mathcal{H})$ felírható $X = A + iB$ alakban, ahol A, B önadjungált. $T(X^*) = T(A - iB) = T(A) - iT(B) = (T(A) + iT(B))^* = T(A + iB)^* = T(X)^*$ miatt ha $T(X) = \lambda X$, akkor $T(X^*) = \overline{\lambda} X^*$.

T és T^* spektruma megegyezik. Ha $0 \leq X$, akkor $X \leq \|X\|_\infty I$ és $0 \leq T^*(I) \leq \|T^*(I)\|_\infty I$ ismételt alkalmazásával

$$0 \leq T^{*n}(X) \leq \|T^*(I)\|_\infty \|X\|_\infty I \tag{3.1}$$

adódik, és így $\|T^{*n}(X)\|_\infty \leq \|T^*(I)\|_\infty \|X\|_\infty$. Tetszőleges $X \in \mathcal{T}(\mathcal{X})$ felírható $X = X_1 + iX_2 - X_3 - iX_4$ alakban, ahol $0 \leq X_i \leq \|X\|_\infty I$, amiből

$$\|T^{*n}(X)\|_\infty \leq 4 \|T^*(I)\|_\infty^n \|X\|_\infty \tag{3.2}$$

és így

$$\varrho(T) = \varrho(T^*) = \lim_{n\to\infty} \sqrt[n]{\|T^{*n}\|_{\infty-\infty}} \leq \lim_{n\to\infty} \sqrt[n]{4 \|T^*(I)\|_\infty^n} = \|T^*(I)\|_\infty \tag{3.3}$$

Ha T nyomőrző, akkor T^* egységőrző, azaz $T^*(I) = 1 \cdot I$, így az 1 sajátérték.

Ha T csatorna, akkor T^n is az, így $\|T^n\|_{1-1} \leq 1$. Legyen J a T lineáris leképezés Jordan-féle normálalakja, erre tehát teljesül, hogy J^n elemei korlátosak amint $n \to \infty$. De ez nem lehetséges, ha $|\lambda| = 1$ és λ-hoz 1×1-nél nagyobb Jordan-blokk tartozik. □

3.2. Definíció. Legyen T Jordan-felbontása

$$T = \sum_{k=1}^{K} (\lambda_k P_k + N_k) \tag{3.4}$$

ahol $P_k P_{k'} = \delta_{kk'} P_k$, $P_k N_{k'} = N_{k'} P_k = \delta_{kk'} N_k$, $N_k^{\operatorname{Tr} P_k} = 0$, $N_k N_{k'} = \delta_{kk'} N_k^2, \sum_k P_k = I$. Definiáljuk a következő lineáris leképezéseket:

$$T_\infty = \sum_{k:\lambda_k=1} P_k \tag{3.5}$$

$$T_\phi = \sum_{k:|\lambda_k|=1} P_k \tag{3.6}$$

$$T_\varphi = \sum_{k:|\lambda_k|=1} \lambda_k P_k \tag{3.7}$$

$$\tag{3.8}$$

3.3. Lemma (Dirichlet tétel)**.** *Legyenek $x_1, \ldots, x_m \in \mathbb{R}$ és $q \in \mathbb{N}+2$. Ekkor léteznek olyan $n, p_1, \ldots, p_m \in \mathbb{Z}$ számok, amelyekre*

$$1 \leq n \leq q^m \text{ és } \forall k \in [m] : |nx_k - p_k| \leq \frac{1}{q} \tag{3.9}$$

teljesül.

Bizonyítás. Tekintsük $[0,1]^m$-et a szemközti oldalakat azonosítva, bontsuk fel $1/q \times \dots \times 1/q$ méretű kockákra. A $(0,\dots,0),(x_1,\dots,x_m),(2x_1,\dots,2x_m),\dots,(q^m x_1,\dots,q^m x_m)$ törtrészei ebben q^m+1 pontot határoznak meg, így van közöttük kettő, ami egy kockába esik. Legyen a kettő különbsége $(nx_1,\dots,nx_m)$. Ennek minden tagja abszolút értékben közelebb van egy egész számhoz mint $1/q$. □

3.4. Állítás. *A fenti jelölésekkel az alábbiak igazak:*

1.
$$T_\infty = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} T^n \tag{3.10}$$

2. *Létezik olyan* $n : \mathbb{N} \to \mathbb{N}$ *növekvő sorozat, amire* $\lim_{i\to\infty} T^{n_i} = T_\phi$
3. $T_\varphi = TT_\phi$

Következésképp $T_\infty, T_\phi, T_\varphi$ *mindegyike csatorna.*

Bizonyítás. **1** Jordan-blokkonként: ha $|\lambda_k| < 1$, akkor

$$\left\| \sum_{n=1}^{N} (\lambda_k P_k + N_k)^n \right\|_1 \le \sum_{n=1}^{\infty} \|(\lambda_k P_k + N_k)^n\|_1 < \infty \tag{3.11}$$

közös korlát, N-nel osztva tehát 0-hoz tart. Ha $|\lambda_k| = 1$, akkor 1×1 Jordan-blokk tartozik hozzá, így ha $\lambda_k = 1$, akkor

$$\frac{1}{N} \sum_{n=1}^{N} (\lambda_k P_k)^n = P_k \tag{3.12}$$

egyébként pedig

$$\left| \frac{1}{N} \sum_{n=1}^{N} \lambda_k^n \right| = \frac{1}{N} \left| \lambda_k \frac{1-\lambda_k^N}{1-\lambda_k} \right| \le \frac{1}{N} \frac{2}{|1-\lambda_k|} \tag{3.13}$$

ami 0-hoz tart.

2 Ha nincs olyan λ_k sajátérték, amire $|\lambda_k|$ és λ_k nem egységgyök, akkor valamilyen N-re T^N minden 1 abszolútértékű sajátértéke 1, ekkor a $T^N, T^{2N}, T^{3N}, \dots$ részsorozat jó. Ellenkező esetben minden $\varepsilon > 0$-hoz létezik olyan n, amire $|\lambda_k^n - 1| < \varepsilon$ minden olyan λ_k sajátértékre, amire $|\lambda_k| = 1$ és lehet olyan $\varepsilon \to 0$ sorozatot találni, amihez tartozó minimális n-ek sorozata növekvő. Egy ilyen n_i sorozatra $T^{n_i} \to T_\phi$.

3 Ha $|\lambda_k| = 1$, akkor $\operatorname{Tr} P_k = 1$ és így $TP_k = \lambda_k P_k$.

□

3.5. Tétel (Nemkommutatív Riesz-Thorin)**.** *Legyen* $T : \mathrm{Mat}(n,\mathbb{C}) \to \mathrm{Mat}(m,\mathbb{C})$ *lineáris leképezés. Ekkor*

$$\|T\|_{p-p} \le \|T\|_{1-1}^{\frac{1}{p}} \|T\|_{\infty-\infty}^{1-\frac{1}{p}} \tag{3.14}$$

3.6. Következmény. *Ha* $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ *egységőrző csatorna, akkor* $p \geq 1$ *esetén* $\|T\|_{p-p} = 1$*.*

Bizonyítás. T és T^* is csatorna, tehát $\|T\|_{1-1} = 1$, $\|T^*\|_{1-1} = 1$. De ekkor $\|T\|_{\infty-\infty} = \|T^*\|_{1-1} = 1$, és így minden p-re $1 \leq \|T\|_{p-p} \leq 1$. □

3.7. Állítás. *Legyen* $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ *pozitív trace-őrző leképezés. Ekkor* $\det T \in [-1, 1]$*. Ha* $|\det T| = 1$*, akkor* $T(\varrho) = U\varrho U^*$ *valamilyen unitér vagy antiunitér operátorra.*

Bizonyítás. Mivel λ és $\overline{\lambda}$ multiplicitása megegyezik, $\det T \in \mathbb{R}$. $\det T$ a sajátértékek szorzata, ezek abszolútértéke kisebb mint 1, így $|\det T| \leq 1$.

Ha $|\det T| = 1$, akkor minden sajátérték abszolútértéke 1, tehát $T_\phi = \mathrm{id}_{\mathcal{T}(\mathcal{H})}$. Vegyünk egy olyan n_i részsorozatot, amire $T^{n_i} \to \mathrm{id}$, ekkor $\lim_{i\to\infty} T^{n_i - 1} = T^{-1}$ is csatorna.

Mivel T és T^{-1} állapotot állapotba, konvex kombinációt konvex kombinációba visz, ϱ pontosan akkor tiszta, ha $T(\varrho)$ tiszta. Másfelől $T(I) = I$, ellenkező esetben ugyanis $T(I)$ legkisebb sajátértékére $\lambda_{\min} < 1$ teljesülne, de ha a hozzá tartozó sajátvektor $|\varphi\rangle$, akkor $I - \frac{\lambda_{\min}+1}{2} T^{-1}(|\varphi\rangle\langle\varphi|)$ pozitív lenne, de T általi képe nem.

T egység- és trace-őrző, tehát kontrakció a Hilbert-Schmidt-normára nézve. Mivel az inverze is ilyen, $\|T(A)\|_2 = \|A\|_2$ minden A-ra igaz. Ekkor $\operatorname{Tr} T(A)^* T(B) = \operatorname{Tr} A^* B$ is teljesül minden A, B-re, legyen $A = |\psi\rangle\langle\psi|$, $B = |\varphi\rangle\langle\varphi|$, ezek képe tiszta, tehát T megszorítva a tiszta állapotokra a projektív Hilbert-tér izometrikus automorfizmusa. Wigner tétele szerint T unitér vagy antiunitér operátorral való konjugálás. □

3.8. Következmény. *Ha* T *invertálható, pozitív és trace-őrző, és az inverze is pozitív, akkor* T *unitér vagy antiunitér operátorral való konjugálás.*

4. Csatorna-félcsoportok

- ha egy zárt rendszer állapota kezdetben ϱ, akkor t idő múlva $U\varrho U^*$ lesz, ahol $U = e^{-iHt}$
- ebben a leírásban az idő „diszkrét", csak a 0 és t pillanat érdekes
- valójában minden $t > 0$-hoz rendelhetünk állapotot: $t \mapsto e^{-iHt}\varrho e^{iHt}$
- másképp: $T_t(\varrho) = e^{-iHt}\varrho e^{iHt}$, itt T_t minden $t \in \mathbb{R}$-re kvantum csatorna, $T_{t+s} = T_t \circ T_s$, $T_0 = \mathrm{id}$
- fizikai megfontolásból / azért, hogy tudjunk valami érdekeset mondani: $t \mapsto T_t$ legyen folytonos
- kérdés: mi a helyzet, ha a rendszerről nem tesszük fel, hogy zárt, csak pl. azt, hogy az időfejlődés Markov és homogén

4.1. Definíció. Legyen $\mathcal{H}$ Hilbert-tér. Egy $\mathbb{R}_+ \ni t \mapsto T_t :\to \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ $\|\cdot\|_{1-1}$-folytonos leképezést kvantum dinamikai félcsoportnak nevezünk, ha minden t-re T_t kvantum csatorna, $T_0 = \mathrm{id}_{\mathcal{T}(\mathcal{H})}$ és $t, s \in \mathbb{R}_+$ esetén $T_{t+s} = T_t \circ T_s$.

- minden kvantum csatorna lineáris leképezés, először csak azt tegyük fel, hogy $T : \mathbb{R}_+ \to \mathrm{Mat}(D, \mathbb{C})$ folytonos (ez jól definiált)

4.2. Állítás. *Legyen $T : \mathbb{R}_+ \to \mathrm{Mat}(D, \mathbb{C})$ folytonos, és tegyük fel, hogy $T_0 = I$ és minden $s, t \in \mathbb{R}_+$ esetén $T_{t+s} = T_t \circ T_s$. Ekkor T differenciálható és $T_t = e^{tL}$ valamilyen $L \in \mathrm{Mat}(D, \mathbb{C})$-re.*

Bizonyítás. Ha $\varepsilon > 0$ elég kicsi, akkor

$$M_\varepsilon := \int_0^\varepsilon T_s ds \tag{4.1}$$

invertálható, másrészt $t \mapsto M_t$ differenciálható, deriváltja T. Alkalmas ε-t rögzítve

$$\begin{aligned} T_t &= M_\varepsilon^{-1} M_\varepsilon T_t \\ &= M_\varepsilon^{-1} \int_0^\varepsilon T_{s+t} ds \\ &= M_\varepsilon^{-1} \int_t^{t+\varepsilon} T_s ds \\ &= M_\varepsilon^{-1} (M_{t+\varepsilon} - M_t) \end{aligned} \tag{4.2}$$

ami differenciálható.

Mindkét oldalt deriválva a

$$\begin{aligned} \frac{d}{dt} T_t &= M_\varepsilon^{-1} (T_{t+\varepsilon} - T_t) \\ &= M_\varepsilon^{-1} (T_\varepsilon - I) T_t \end{aligned} \tag{4.3}$$

differenciálegyenletet kapjuk, aminek megoldása $T_t = e^{tL}$, ahol $L = M_\varepsilon^{-1} (T_\varepsilon - I)$. □

Megjegyzés. Az állítás igaz marad végtelen dimenzióban is, ha operátor-normában folytonosságot teszünk fel, ekkor L korlátos.

- egy folytonos dinamikai félcsoportot tehát a generátorával egyértelműen jellemezhetünk
- mi történik, ha kicsit megváltoztatjuk a generátort?

4.3. Lemma. *Legyen $T_t = e^{tL}, T'_t = e^{tL'}$ és $\Delta = L' - L$. Ekkor minden t-re*

$$T'_t - T_t = \int_0^t T_{t-s} \Delta T'_s ds \tag{4.4}$$

Bizonyítás. Legyen $f(s) = T_{t-s}T'_s$, ennek deriváltja $f'(s) = T_{t-s}(L' - L)T'_s$ és

$$T'_t - T_t = f(t) - f(0) = \int_0^t f'(s)ds = \int_0^t T_{t-s}\Delta T'_s ds \tag{4.5}$$

□

4.4. Következmény. *Legyen $T_t = e^{tL}, T'_t = e^{tL'}$ és $\Delta = L' - L$. Ekkor*

$$\|T'_t - T_t\| \leq t\,\|\Delta\| \sup_{s,s' \in [0,t]} \|T_s\|\,\|T'_{s'}\| \tag{4.6}$$

bármely $\|\cdot\|$ indukált operátornorma esetén.

- mostantól feltesszük, hogy T_t kvantum csatorna
- mit lehet ekkor mondani a generátorról?

4.5. Állítás. *Legyen $L : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ lineáris leképezés. A következők ekvivalensek:*

1. *Létezik olyan $\Phi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ teljesen pozitív leképezés és $\kappa \in \mathcal{B}(\mathcal{H})$, hogy minden $\varrho \in \mathcal{T}(\mathcal{H})$ esetén*

$$L(\varrho) = \Phi(\varrho) - \kappa\varrho - \varrho\kappa^* \tag{4.7}$$

2. *L önadjungált operátorokat önadjungáltba képez, és ha $|\Omega\rangle \in \mathcal{H} \otimes \mathcal{H}$ egy tetszőleges teljesen összefont állapotvektor, $P = \mathrm{id}_{\mathcal{H}\otimes\mathcal{H}} - |\Omega\rangle\langle\Omega|$, akkor*

$$P(L \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H})})(|\Omega\rangle\langle\Omega|)P \geq 0 \tag{4.8}$$

Bizonyítás. **1 $\Longrightarrow$ 2**

$$\begin{aligned} P(L \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^d)})(|\Omega\rangle\langle\Omega|)P =& P(\Phi \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^d)})(|\Omega\rangle\langle\Omega|)P \\ & - P(\kappa \otimes I)|\Omega\rangle\langle\Omega|P - P|\Omega\rangle\langle\Omega|(\kappa^* \otimes I)P \\ =& P(\Phi \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^d)})(|\Omega\rangle\langle\Omega| \end{aligned} \tag{4.9}$$

pozitív, mivel Φ teljesen pozitív. $L(\varrho^*) = \Phi(\varrho^*) - \varrho^*\kappa^* - \kappa\varrho^* = L(\varrho)^*$.

2 $\Longrightarrow$ 1 $\tau := (L \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^d)})(|\Omega\rangle\langle\Omega|)$ önadjungált, $P\tau P \geq 0$ miatt $\tau = Q - |\psi\rangle\langle\Omega| - |\Omega\rangle\langle\psi|$, ahol $Q \geq 0$ és $Q|\Omega\rangle = 0$. Létezik olyan teljesen pozitív leképezés, amire $(\Phi \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^d)})(|\Omega\rangle\langle\Omega|) = Q$, legyen κ olyan, hogy $(\kappa \otimes I)|\Omega\rangle = |\psi\rangle$.

□

4.6. Definíció. Egy $L : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ lineáris leképezés feltételes teljesen pozitív, ha teljesíti az előző állítás ekvivalens feltételeit.

4.7. Állítás. *Legyen minden $t \in \mathbb{R}_+$-ra $T_t : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ lineáris leképezés. A következők ekvivalensek:*

1. *$t \mapsto T_t$ teljesen pozitív leképezések folytonos egyparaméteres félcsoportja*
2. *$T_t = e^{tL}$ valamely $L : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ feltételes teljesen pozitív leképezésre*

Bizonyítás. **1 $\Longrightarrow$ 2** Létezik $L : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ generátor, amire $T_t = e^{tL}$. Mivel T_t minden t-re teljesen pozitív, kis t-re és teljesen összefont $|\Omega\rangle\langle\Omega|$-ra:

$$\begin{aligned} 0 &\leq (e^{tL} \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H})})(|\Omega\rangle\langle\Omega|) \\ &= |\Omega\rangle\langle\Omega| + t(L \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H})})(|\Omega\rangle\langle\Omega|) + o(t) \end{aligned} \tag{4.10}$$

$P = I - |\Omega\rangle\langle\Omega|$-vel mindkét oldalról szorozva, t-vel osztva majd $t \to 0$ határátmenet után látjuk, hogy L feltételes teljesen pozitív.

2 $\Longrightarrow$ 1 e^{tL} folytonos egyparaméteres félcsoport. Legyen $\Phi_\kappa(\varrho) = -\kappa\varrho - \varrho\kappa^*$, ekkor $L = \Phi + \Phi_\kappa$. Mivel

$$e^{tL} = \lim_{n\to\infty} \left(e^{t\Phi/n} e^{t\Phi_\kappa/n}\right)^n \tag{4.11}$$

elég azt látni, hogy $e^{t\Phi/n}$ és $e^{t\Phi_\kappa/n}$ teljesen pozitív.

Φ teljesen pozitív, ezért

$$e^{t\Phi/n} = \sum_{k=0}^{\infty} \left(\frac{t}{n}\right)^k \frac{\Phi^k}{k!} \tag{4.12}$$

is az.

$$e^{t\Phi_\kappa/n}(\varrho) = e^{-t\kappa/n}\varrho e^{t\kappa/n} = e^{-t\kappa/n}\varrho \left(e^{-t\kappa/n}\right)^* \tag{4.13}$$

miatt ez is teljesen pozitív.

□

4.8. Állítás. *Legyen $L(\varrho) = \Phi(\varrho) - \kappa\varrho - \varrho\kappa^*$, ahol $\Phi(\varrho) = \sum_i L_i\varrho L_i^*$. Legyen $c_i \in \mathbb{C}$, $\lambda \in \mathbb{R}$ és*

$$L_i' = L_i + c_i I \tag{4.14}$$

$$\kappa' = \kappa + \sum_i \overline{c_i} L_i + i\lambda I + \frac{1}{2}\sum_i |c_i|^2 I \tag{4.15}$$

Ekkor $L(\varrho) = \Phi'(\varrho) - \kappa'\varrho - \varrho\kappa'^*$, ahol $\Phi'(\varrho) = \sum_i L_i'\varrho L_i'^*$

Bizonyítás.

$$\begin{aligned}
&\Phi'(\varrho) - \kappa'\varrho - \varrho\kappa'^* \\
&= \sum_i L_i'\varrho L_i'^* - \kappa'\varrho - \varrho\kappa'^* \\
&= \sum_i \Big(L_i\varrho L_i^* + c_i\varrho L_i^* + \overline{c_i}L_i\varrho + |c_i|^2\varrho\Big) - \kappa\varrho - \sum_i \overline{c_i}L_i\varrho \\
-i\lambda\varrho - \frac{1}{2}\sum_i |c_i|^2\varrho - \varrho\kappa^* - \sum_i c_i\varrho L_i^* + i\lambda\varrho - \frac{1}{2}\sum_i |c_i|^2\varrho \\
&= \sum_i L_i\varrho L_i^* - \kappa\varrho - \varrho\kappa^* = L(\varrho)
\end{aligned} \tag{4.16}$$

□

4.9. Állítás. *Legyen* $L(\varrho) = \Phi(\varrho) - \kappa\varrho - \varrho\kappa^* = \Phi'(\varrho) - \kappa'\varrho - \varrho\kappa'^*$ *mint eddig, és tegyük fel, hogy* Φ *és* Φ' *Kraus-operátorainak mindegyike* 0 *nyomú. Ekkor* $\Phi = \Phi'$ *és* $\kappa = \kappa' + i\lambda I$ *valamilyen* $\lambda \in \mathbb{R}$*-re.*

Bizonyítás. Legyen $|\Omega\rangle = \sum_i |i\rangle \otimes |i\rangle$ teljesen összefont állapot, ekkor $(L \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H})})(|\Omega\rangle\langle\Omega|)$ meghatározza L-t. Az első tagot külön tekintve:

$$\begin{aligned}
\langle\Omega|(\Phi \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H})})(|\Omega\rangle\langle\Omega|) &= \sum_{i_1 i_2 i_3 j} (\langle i_1| \otimes \langle i_1|)(K_j|i_2\rangle\langle i_3|K_j^* \otimes |i_2\rangle\langle i_3|) \\
&= \sum_{i_1 i_3 j} (\langle i_1|K_j|i_1\rangle\langle i_3|K_j^* \otimes \langle i_3| \\
&= \sum_{i_3 j} \operatorname{Tr} K_j\langle i_3|K_j^* \otimes \langle i_3| = 0
\end{aligned} \tag{4.17}$$

és $(\Phi\otimes\mathrm{id}_{\mathcal{T}(\mathcal{H})})(|\Omega\rangle\langle\Omega|)|\Omega\rangle = 0$, mivel ennek az adjungáltja. Ha viszont $\psi \perp \Omega$ és $\varphi \perp \Omega$, akkor

$$\langle\psi|(\kappa \otimes I)(|\Omega\rangle\langle\Omega|)|\varphi\rangle = 0 \tag{4.18}$$

$$\langle\psi|(|\Omega\rangle\langle\Omega|)(\kappa^* \otimes I)|\varphi\rangle = 0 \tag{4.19}$$

Minden $\mathcal{H}\otimes\mathcal{H} \to \mathcal{H}\otimes\mathcal{H}$ önadjungált lineáris leképezés egyértelműen kettő olyan összegére, amelyek közül az első magja tartlmazza Ω-t, a második pedig $\Omega^\perp$ projektorával két oldalról komponálva 0-t ad. Emiatt $\Phi(\varrho) = \Phi'(\varrho)$ és $\kappa\varrho + \varrho\kappa^* = \kappa'\varrho + \varrho\kappa'^*$ minden ϱ-ra, azaz $(\kappa - \kappa')\varrho + \varrho(\kappa - \kappa')^* = 0$, amiből $\kappa - \kappa' = i\lambda I$ valamilyen $\lambda \in \mathbb{R}$-re. □

11. HF. Legyen $L : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{H})$ lineáris leképezés. Ekkor a következők ekvivalensek:

1. L egy kvantum dinamikai félcsoport generátora
2. $L(\varrho) = \Phi(\varrho) - \kappa\varrho - \varrho\kappa^*$, ahol Φ teljesen pozitív, $\Phi^*(I) = \kappa + \kappa^*$

3.
$$L(\varrho) = i[\varrho, H] + \sum_i \left(L_i \varrho L_i^* - \frac{1}{2}\{L_i^* L_i, \varrho\} \right) \tag{4.20}$$

4.
$$L(\varrho) = i[\varrho, H] + \frac{1}{2} \sum_i \left([L_i, \varrho L_i^*] + [L_i \varrho, L_i^*] \right) \tag{4.21}$$

ahol $H = H^* = \frac{\kappa - \kappa^*}{2i}$, és L_i a Φ Kraus-operátorai.

- H (κ képzetes része) a Hamilton-operátor, ez az időfejlődés koherens részét határozza meg
- az összes energiaszint eltolása nem változtatja meg a dinamikát
- Φ és κ valós része (ezt Φ meghatározza!) a dinamika inkoherens vagy disszipatív része
- ez a felbontás nem egyértelmű, de ha kikötjük, hogy a Kraus-operátorok nyoma 0, akkor már az
- Φ Kraus-operátorait Lindblad-operátoroknak nevezzük

5. Entrópiák

- entrópiák: olyan mennyiségek, amelyek egy állapot (vagy klasszikus eloszlás) által hordozott „bizonytalanságot”, „rendezetlenséget” jellemzik
- pl. $P_X : \mathcal{X} \to [0, 1]$ diszkrét eloszlás Shannon-entrópiája

$$H(X)_P \equiv H(P_X) = -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x) \tag{5.1}$$

- pl. ha P_X egyenletes eloszlás, akkor $H(P_X) = \log |\mathcal{X}|$, ha $P_X(x_0) = 1$, akkor $H(P_X) = 0$
- motiváció: $X_1, \ldots, X_n$ független P_X eloszlású, akkor létezik $nH(P_X) + o(n)$ bites kódolás úgy, hogy a sikertelen dekódolás valószínűsége $o(1)$, de minden rövidebb kódolásnál $1 - o(1)$ ez a valószínűség

5.1. Definíció. Egy $\varrho_X \in \mathcal{S}(\mathcal{H}_X)$ állapot Neumann-entrópiája $H(X)_\varrho \equiv H(\varrho_X) = -\operatorname{Tr} \varrho_X \log \varrho_X$.

- feltételes entrópiák: bizonytalanság egy másik (pl. a vizsgálttal korrelált) valószínűségi változó ismeretében
- pl. $P = P_{XY} : \mathcal{X} \times \mathcal{Y} \to [0, 1]$ diszkrét eloszlás

$$\begin{aligned} H(X|Y)_P &= H(XY)_P - H(Y)_P \\ &= -\sum_{y \in \mathcal{Y}} P_Y(y) \sum_{x \in \mathcal{X}} P_{X|Y}(x|y) \log P_{X|Y}(x|y) \end{aligned} \tag{5.2}$$

- pl. X és Y független, akkor $H(X|Y)_P = H(X)_P$ (spec: $\mathcal{Y} = 1$, akkor függetlenek)
- pl. $\mathcal{X} = \mathcal{Y}$ és $P(X = Y) = 1$, akkor $H(X|Y)_P = 0$
- motiváció: $(X_1, Y_1), \ldots, (X_n, Y_n)$ független P_{XY} eloszlású, akkor létezik $nH(P_X|P_Y) + o(n)$ bites kódolás úgy, hogy Y ismeretében a sikertelen dekódolás valószínűsége $o(1)$, de minden rövidebb kódolásnál $1 - o(1)$ ez a valószínűség

5.2. Definíció. Egy $\varrho \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_Y)$ állapot feltételes entrópiája $H(X|Y)_\varrho = H(XY)_\varrho - H(Y)_\varrho$.

- kölcsönös információ: két valószínűségi változó függőségét jellemzi
- pl. $P = P_{XY} : \mathcal{X} \times \mathcal{Y} \to [0, 1]$ diszkrét eloszlás

$$
\begin{aligned}
I(X;Y)_P &= H(X)_P - H(X|Y)_P \\
&= H(X)_P + H(Y)_P - H(XY)_P \\
&= \sum_{\substack{x \in \mathcal{X} \\ y \in \mathcal{Y}}} P_{XY}(x, y) \log \frac{P_{XY}(x, y)}{P_X(x) P_Y(y)}
\end{aligned}
\tag{5.3}
$$

- pl. X és Y független, akkor $I(X;Y)_P = 0$
- pl. $\mathcal{X} = \mathcal{Y}$ és $P(X = Y) = 1$, akkor $I(X;Y)_P = H(X)_P$

5.3. Definíció. Egy $\varrho \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_Y)$ állapot kölcsönös információja $I(X;Y)_\varrho = H(X)_\varrho + H(Y)_\varrho - H(XY)_\varrho$.

Egy $\varrho \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_Z)$ állapot feltételes kölcsönös információja $I(X;Y|Z)_\varrho = H(X|Z)_\varrho + H(Y|Z)_\varrho - H(XY|Z)_\varrho$.

- relatív entrópiák: két különböző állapot eltérését mérik (általában nem szimmetrikus módon)
- pl. $P, Q : \mathcal{X} \to [0, 1]$ két diszkrét eloszlás

$$
D(P||Q) = \sum_{x \in \mathcal{X}} P(x) \log \frac{P(x)}{Q(x)}
\tag{5.4}
$$

- pl. $P = Q$, akkor $D(P||Q) = 0$

5.4. Definíció. A $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$ állapotok közötti relatív entrópia

$$
D(\varrho||\sigma) = \operatorname{Tr} \varrho(\log(\varrho) - \log(\sigma))
\tag{5.5}
$$

5.5. Állítás. *Legyen $\varrho_{XA} \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_A)$ klasszikus-kvantum, azaz*

$$
\varrho_{XA} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \varrho_x
\tag{5.6}
$$

Ekkor

$$H(XA)_\varrho = H(X)_\varrho + \sum_{x\in\mathcal{X}} P_X(x) H(A)_{\varrho_x} \tag{5.7}$$

és

$$H(A|X)_\varrho = \sum_{x\in\mathcal{X}} P_X(x) H(A)_{\varrho_x} \tag{5.8}$$

Bizonyítás.

$$\begin{aligned}
H(XA)_\varrho &= -\operatorname{Tr} \varrho_{XA} \log \varrho_{XA} \\
&= -\operatorname{Tr} \left(\sum_{x\in\mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \varrho_x \right) \\
&\quad \cdot \left(\sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes (\log P_X(x) I + \log \varrho_x) \right) \\
&= -\sum_{x\in\mathcal{X}} P_X(x) \operatorname{Tr} \varrho_x \log P_X(x) \\
&\quad - \sum_{x\in\mathcal{X}} P_X(x) \operatorname{Tr} \varrho_x \log \varrho_x \\
&= H(X)_\varrho + \sum_{x\in\mathcal{X}} P_X(x) H(A)_{\varrho_x}
\end{aligned} \tag{5.9}$$

és

$$H(A|X)_\varrho = H(XA)_\varrho - H(X)_\varrho = \sum_{x\in\mathcal{X}} P_X(x) H(A)_{\varrho_x} \tag{5.10}$$

□

5.6. Állítás. *Legyen $\varrho \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_A \otimes \mathcal{H}_B)$ klasszikus-kvantum-kvantum, azaz*

$$\varrho_{XAB} = \sum_{x\in\mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \varrho_x \tag{5.11}$$

ahol $\varrho_x \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ $(x \in \mathcal{X})$. Ekkor

$$I(A;B|X)_\varrho = \sum_{x\in\mathcal{X}} P_X(x) I(A;B)_{\varrho_x} \tag{5.12}$$

Bizonyítás.

$$\begin{aligned}
I(A;B|X)_\varrho &= H(A|X)_\varrho + H(B|X)_\varrho - H(AB|X)_\varrho \\
&= \sum_{x\in\mathcal{X}} P_X(x) H(A)_{\varrho_x} + \sum_{x\in\mathcal{X}} P_X(x) H(B)_{\varrho_x} \\
&\quad - \sum_{x\in\mathcal{X}} P_X(x) H(AB)_{\varrho_x} \\
&= \sum_{x\in\mathcal{X}} P_X(x) I(A;B)_{\varrho_x}
\end{aligned} \tag{5.13}$$

□

12. HF. Legyenek $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_A)$ klasszikus-kvantum állapotok, azaz

$$\varrho_{XA} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \varrho_x \sigma_{XA} \qquad = \sum_{x\in\mathcal{X}} Q_X(x)|x\rangle\langle x| \otimes \sigma_x \tag{5.14}$$

Ekkor

$$D(\varrho||\sigma) = D(P||Q) + \sum_{x\in\mathcal{X}} P_X(x) D(\varrho_x||\sigma_x) \tag{5.15}$$

5.7. Állítás. *Legyen* $\varrho_{A_1\dots A_n} \in \mathcal{S}(\mathcal{H}_{A_1} \otimes \dots \otimes \mathcal{H}_{A_n})$. *Ekkor*

$$H(A_1 \dots A_n)_\varrho = H(A_1)_\varrho + H(A_2|A_1)_\varrho + \dots + H(A_n|A_1 \dots A_{n-1})_\varrho \tag{5.16}$$

Bizonyítás.

$$\begin{aligned} &H(A_1)_\varrho + H(A_2|A_1)_\varrho + \dots + H(A_n|A_1 \dots A_{n-1})_\varrho \\ &\quad = H(A_1)_\varrho + H(A_1A_2)_\varrho - H(A_1)_\varrho + H(A_1A_2A_3)_\varrho - H(A_1A_2)_\varrho \\ &\qquad + \dots + H(A_1A_2 \dots A_n)_\varrho - H(A_1 \dots A_{n-1})_\varrho \\ &\qquad\qquad = H(A_1A_2 \dots A_n)_\varrho \end{aligned} \tag{5.17}$$

□

13. HF. Legyen $\varrho_{A_1\dots A_nB} \in \mathcal{S}(\mathcal{H}_{A_1} \otimes \dots \otimes \mathcal{H}_{A_n} \otimes \mathcal{H}_B)$. Ekkor

$$I(A_1 \dots A_n; B)_\varrho = I(A_1; B)_\varrho + I(A_2; B|A_1)_\varrho + \dots + I(A_n; B|A_1 \dots A_{n-1})_\varrho \tag{5.18}$$

5.8. Állítás. *Legyen* $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$. *Ekkor*

$$H(A|B)_\varrho = \log \dim \mathcal{H}_A - D\left(\varrho_{AB}||\frac{\mathrm{id}_{\mathcal{H}_A}}{\dim \mathcal{H}_A} \otimes \varrho_B\right) \tag{5.19}$$

és

$$I(A;B)_\varrho = D(\varrho_{AB}||\varrho_A \otimes \varrho_B) \tag{5.20}$$

Bizonyítás.

$$\begin{aligned} &D\left(\varrho_{AB}||\frac{\mathrm{id}_{\mathcal{H}_A}}{\dim \mathcal{H}_A} \otimes \varrho_B\right) \\ &= \mathrm{Tr}\left(\varrho_{AB}(\log \varrho_{AB} - \log\left(\frac{\mathrm{id}_{\mathcal{H}_A}}{\dim \mathcal{H}_A} \otimes \varrho_B\right))\right) \\ &= \mathrm{Tr}(\varrho_{AB} \log \varrho_{AB}) \\ &\quad - \mathrm{Tr}\left(\varrho_{AB}\left(\log \frac{\mathrm{id}_{\mathcal{H}_A}}{\dim \mathcal{H}_A} \otimes \mathrm{id}_{\mathcal{H}_B} + \mathrm{id}_{\mathcal{H}_A} \otimes \log \varrho_B\right)\right) \\ &= - H(\varrho_{AB}) + \log \dim \mathcal{H}_A + H(\varrho_B) \\ &= \log \dim \mathcal{H}_A - H(A|B)_\varrho \end{aligned} \tag{5.21}$$

$$\begin{aligned}
&D\left(\varrho_{AB}||\varrho_A \otimes \varrho_B\right) \\
&= \mathrm{Tr}(\varrho_{AB}(\log \varrho_{AB} - \log(\varrho_A \otimes \varrho_B))) \\
&= \mathrm{Tr}(\varrho_{AB} \log \varrho_{AB}) - \mathrm{Tr}(\varrho_{AB}(\log \varrho_A \otimes I + I \otimes \log \varrho_B)) \\
&= -H(\varrho_{AB}) + H(\varrho_A) + H(\varrho_B) \\
&= I(A;B)_\varrho
\end{aligned} \tag{5.22}$$

□

5.9. Állítás. *Legyen* $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$, $U : \mathcal{H} \to \mathcal{K}$ *izometria. Ekkor* $D(U\varrho U^*||U\sigma U^*) = D(\varrho||\sigma)$.

Bizonyítás.

$$\begin{aligned}
D(U\varrho U^*||U\sigma U^*) &= \mathrm{Tr}(U\varrho U^*(\log(U\varrho U^*) - \log(U\sigma U^*))) \\
&= \mathrm{Tr}(U\varrho U^*(U\log(\varrho)U^* - U\log(\sigma)U^*)) \\
&= \mathrm{Tr}(\varrho(\log(\varrho) - \log(\sigma))) \\
&= D(\varrho||\sigma)
\end{aligned} \tag{5.23}$$

□

5.10. Következmény. *Ha* $U_A : \mathcal{H}_A \to \mathcal{K}_A$ *és* $U_B : \mathcal{H}_B \to \mathcal{K}_B$ *izometriák,* $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, *akkor* $H(A|B)_{\varrho_{AB}} = H(A|B)_{(U_A\otimes U_B)\varrho_{AB}(U_A\otimes U_B)^*}$ *és* $I(A;B)_{\varrho_{AB}} = I(A;B)_{(U_A\otimes U_B)\varrho_{AB}(U_A\otimes U_B)^*}$.

5.11. Következmény. *Ha* $U : \mathcal{H} \to \mathcal{K}$ *izometria,* $\varrho \in \mathcal{S}(\mathcal{H})$, *akkor* $H(\varrho) = H(U\varrho U^*)$.

5.12. Következmény. *Ha* $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ *tiszta, akkor* $H(\varrho_A) = H(\varrho_B)$.

5.13. Következmény. *Ha* $\varrho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ *tiszta, akkor* $H(A|B)_\varrho = -H(A|C)_\varrho$.

Bizonyítás.

$$\begin{aligned}
H(A|B)_\varrho + H(A|C)_\varrho &= H(AB)_\varrho - H(B)_\varrho + H(AC)_\varrho - H(C)_\varrho \\
&= H(AB)_\varrho - H(C)_\varrho + H(AC)_\varrho - H(B)_\varrho \\
&= 0
\end{aligned} \tag{5.24}$$

□

5.14. Állítás. *Legyen* $\varrho_1, \sigma_1 \in \mathcal{S}(\mathcal{H}_1)$ *és* $\varrho_2, \sigma_2 \in \mathcal{S}(\mathcal{H}_2)$. *Ekkor* $D(\varrho_1 \otimes \varrho_2||\sigma_1 \otimes \sigma_2) = D(\varrho_1||\sigma_1) + D(\varrho_2||\sigma_2)$.

Bizonyítás.

$$\begin{aligned}
&D(\varrho_1 \otimes \varrho_2 || \sigma_1 \otimes \sigma_2) \\
&= \mathrm{Tr}((\varrho_1 \otimes \varrho_2)(\log(\varrho_1 \otimes \varrho_2) - \log(\sigma_1 \otimes \sigma_2))) \\
&= \mathrm{Tr}((\varrho_1 \otimes \varrho_2)(\log \varrho_1 \otimes I + I \otimes \log \varrho_2 \\
&\qquad - \log \sigma_1 \otimes I - I \otimes \log \sigma_2))) \\
&= \mathrm{Tr}(\varrho_1(\log \varrho_1 - \log \sigma_1)) + \mathrm{Tr}(\varrho_2(\log \varrho_2 - \log \sigma_2)) \\
&= D(\varrho_1 || \sigma_1) + D(\varrho_2 || \sigma_2)
\end{aligned} \tag{5.25}$$

□

5.15. Következmény. *Ha* $\varrho_1 \in \mathcal{S}(\mathcal{H}_1)$ *és* $\varrho_2 \in \mathcal{S}(\mathcal{H}_2)$, *akkor* $H(\varrho_1 \otimes \varrho_2) = H(\varrho_1) + H(\varrho_2)$

5.16. Következmény. *Ha* $\varrho_{AB} = \varrho_A \otimes \varrho_B \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, *akkor* $H(A|B)_\varrho = H(A)_\varrho$

5.17. Következmény. *Ha* $\dim \mathcal{H}_B = 1$, *akkor* $H(A|B)_\varrho = H(A)_\varrho$.

5.18. Definíció. $f : (a, b) \to \mathbb{R}$ operátorkonvex, ha minden $A = A^*, B = B^* \in \mathcal{B}(\mathbb{C}^n)$, $\lambda \in [0, 1]$ esetén

$$f(\lambda A + (1 - \lambda)B) \le \lambda f(A) + (1 - \lambda) f(B) \tag{5.26}$$

teljesül.

5.19. Lemma. *Az* $f : \mathbb{R}_+ \to \mathbb{R}$, $f(x) = -\log x$ *függvény operátorkonvex.*

Bizonyítás. Ha A és B pozitív és invertálható, akkor $x \mapsto x^{-1}$ konvexitása miatt $0 \le \lambda \le 1$ esetén

$$\left(\lambda I + (1 - \lambda) A^{-1/2} B A^{-1/2}\right)^{-1} \le \lambda I + (1 - \lambda) \left(A^{-1/2} B A^{-1/2}\right)^{-1} \tag{5.27}$$

amiből

$$\begin{aligned}
&(\lambda A + (1 - \lambda)B)^{-1} \\
&= A^{-1/2} \left(\lambda I + (1 - \lambda) A^{-1/2} B A^{-1/2}\right)^{-1} A^{-1/2} \\
&\le A^{-1/2} \left(\lambda I + (1 - \lambda) \left(A^{-1/2} B A^{-1/2}\right)^{-1}\right) A^{-1/2} \\
&= \lambda A^{-1} + (1 - \lambda) B^{-1}
\end{aligned} \tag{5.28}$$

$$-\log x = \int_0^\infty \left(\frac{1}{a + t} - \frac{1}{1 + t}\right) dt \tag{5.29}$$

miatt

$$-\log A = \int_0^\infty \left((A + tI)^{-1} - (I + tI)^{-1}\right) dt \tag{5.30}$$

és így

$$
\begin{aligned}
& -\log(\lambda A+(1-\lambda)B) \\
& = \int_0^\infty \Big(((\lambda A+(1-\lambda)B)+tI)^{-1}-(I+tI)^{-1}\Big)\,dt \\
& = \int_0^\infty \Big((\lambda(A+tI)+(1-\lambda)(B+tI))^{-1}-(I+tI)^{-1}\Big)\,dt \qquad (5.31)\\
& \le \int_0^\infty \Big((\lambda(A+tI)^{-1}+(1-\lambda)(B+tI)^{-1})-(I+tI)^{-1}\Big)\,dt \\
& = -\lambda\log A-(1-\lambda)\log B
\end{aligned}
$$

□

5.20. Lemma. *Ha $f:(a,b)\to\mathbb{R}$ operátorkonvex, $U:\mathcal{H}\to\mathcal{K}$ izometria, $X=X^*\in\mathcal{B}(\mathcal{K})$ és $\operatorname{spec} X\subseteq(a,b)$ akkor $f(U^*XU)\le U^*f(X)U$.*

Bizonyítás. Legyen $P=UU^*$ és $Q=I_{\mathcal{K}}-P$. Ekkor $U:\mathcal{H}\to\operatorname{ran}P$ unitér és $PU=U$, emiatt

$$
f(U^*XU)=f(U^*P(PXP)PU)=U^*Pf(PXP)PU \qquad (5.32)
$$

Mivel PXP és QXQ tartói ortogonálisak egymásra, $f(PXP+QXQ)=f(PXP)+f(QXQ)$ és $Pf(QXQ)P=0$. $S:=P-Q$ unitér, emiatt

$$
\begin{aligned}
f(PXP+QXQ) &= f\left(\frac{X+SXS^*}{2}\right) \\
&\le \frac{1}{2}f(X)+\frac{1}{2}f(SXS^*) \\
&= \frac{1}{2}f(X)+\frac{1}{2}Sf(X)S^* \\
&= Pf(X)P+Qf(X)Q
\end{aligned} \qquad (5.33)
$$

tehát $Pf(PXP)P=Pf(PXP+QXQ)P\le Pf(X)P$. Emiatt

$$
f(U^*XU)=U^*Pf(PXP)PU\le U^*Pf(X)PU=U^*f(X)U \qquad (5.34)
$$

□

5.21. Lemma. *Legyen $\varrho,\sigma\in\mathcal{S}(\mathcal{H})$ invertálható, $\Delta:\mathcal{HS}(\mathcal{H})\to\mathcal{HS}(\mathcal{H})$, $\Delta(X)=\sigma X\varrho^{-1}$ (relatív moduláris operátor). Ekkor*

$$
D(\varrho||\sigma)=\langle\varrho^{1/2},-\log(\Delta)(\varrho^{1/2})\rangle_{HS} \qquad (5.35)
$$

Bizonyítás. Legyen $L,R:\mathcal{HS}(\mathcal{H})\to\mathcal{HS}(\mathcal{H})$ az $L(X)=\sigma X$, $R(X)=X\varrho^{-1}$ definiálva. Mivel $X\ne0$ esetén $\langle X,L(X)\rangle=\operatorname{Tr}(X^*\sigma X)>0$ és $\langle X,R(X)\rangle=\operatorname{Tr}(X^*X\varrho^{-1})>0$, ezért L és R szigorúan pozitív. Mivel kommutálnak, $\Delta=LR$ is szigorúan pozitív, így létezik logaritmusa és

$\log\Delta = \log L + \log R$. $L^n(X) = \sigma^n X$ felhasználásával $(\log L)(X) = (\log\sigma)X$ és hasonlóan $(\log R)(X) = -X\log\varrho$, tehát

$$\begin{aligned} &\langle \varrho^{1/2}, -\log(\Delta)(\varrho^{1/2})\rangle_{HS} \\ &= -\langle \varrho^{1/2}, \log(L)(\varrho^{1/2}) + \log(R)(\varrho^{1/2})\rangle_{HS} \\ &= -\operatorname{Tr}\left(\varrho^{1/2}((\log\sigma)\varrho^{1/2} - \varrho^{1/2}(\log\varrho))\right) \\ &= \operatorname{Tr}\varrho(\log\varrho - \log\sigma) \end{aligned} \tag{5.36}$$

□

5.22. Tétel. *Legyen $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$ és $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna. Ekkor $D(T(\varrho)||T(\sigma)) \leq D(\varrho||\sigma)$*

Bizonyítás. Először tekinsük azt a speciális esetet, amikor T egy parciális trace, azaz bizonyítsuk be, hogy $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ esetén $D(\varrho_{AB}||\sigma_{AB}) \geq D(\varrho_A||\sigma_A)$.

Tegyük fel, hogy ϱ és σ invertálható, ekkor $D(\varrho||\sigma) = \langle \varrho^{1/2}, -\log(\Delta_{AB})(\varrho^{1/2})\rangle_{HS}$ és $D(\varrho_A||\sigma_A) = \langle \varrho_A^{1/2}, -\log(\Delta_A)(\varrho_A^{1/2})\rangle_{HS}$ a fenti lemma szerinti Δ_A és Δ_{AB} operátorokkal.

Legyen $U : \mathcal{HS}(\mathcal{H}_A) \to \mathcal{HS}(\mathcal{H}_A \otimes \mathcal{H}_B)$ az

$$U(X) = ((X\varrho_A^{-1/2}) \otimes I_B)\varrho_{AB}^{1/2} \tag{5.37}$$

módon megadott leképezés. Ekkor

$$\begin{aligned} \langle X, U^*(Y)\rangle &= \langle U(X), Y\rangle \\ &= \operatorname{Tr}\left(\left((X\varrho_A)^{-1/2} \otimes I_B\right)\varrho_{AB}^{1/2}\right)^* Y \\ &= \operatorname{Tr}\left(\left(\varrho_A^{12}X^*\right) \otimes I_B\right) Y\varrho_{AB}^{1/2} \\ &= \operatorname{Tr} X^* \operatorname{Tr}_B(Y\varrho_{AB}^{1/2})\varrho_A^{-1/2} \end{aligned} \tag{5.38}$$

alapján

$$U^*(Y) = \operatorname{Tr}_B(Y\varrho_{AB}^{1/2})\varrho_A^{-1/2} \tag{5.39}$$

és így

$$\begin{aligned} U^*U(X) &= U^*\left(\left((X\varrho_A^{-1/2}) \otimes I_B\right)\varrho_{AB}^{1/2}\right) \\ &= \operatorname{Tr}_B\left(\left((X\varrho_A^{-1/2}) \otimes I_B\right)\varrho_{AB}^{1/2}\varrho_{AB}^{1/2}\right)\varrho_A^{-1/2} \\ &= X\varrho_A^{-1/2}\left(\operatorname{Tr} B\varrho_{AB}\right)\varrho_A^{-1/2} = X \end{aligned} \tag{5.40}$$

valamint

$$\begin{aligned} U^*\Delta_{AB}U(X) &= U^*\Delta_{AB}\left(\left((X\varrho_A^{-1/2}) \otimes I_B\right)\varrho_{AB}^{1/2}\right) \\ &= U^*\left(\sigma_{AB}\left((X\varrho_A^{-1/2}) \otimes I_B\right)\varrho_{AB}^{1/2}\varrho_{AB}^{-1}\right) \\ &= \operatorname{Tr}_B\left(\sigma_A B\left((X\varrho_A^{-1/2}) \otimes I_B\right)\varrho_{AB}^{-1/2}\varrho_{AB}^{1/2}\right)\varrho_A^{-1/2} \\ &= (\operatorname{Tr}_B \sigma_{AB})\, X\varrho_A^{-1/2}\varrho_A^{-1/2} = \Delta_A(X) \end{aligned} \tag{5.41}$$

azaz $U^*U = \mathrm{id}_{\mathcal{HS}(\mathcal{H}_A)}$ és $U^*\Delta_{AB}U = \Delta_A$ teljesül. Továbbá

$$U(\varrho_A^{1/2}) = (\varrho_A^{1/2}\varrho_A^{-1/2} \otimes I_B)\varrho_{AB}^{1/2} = \varrho_{AB}^{1/2} \tag{5.42}$$

Használva $x \mapsto -\log x$ operátorkonvexitását és a fenti lemmát kapjuk, hogy

$$\begin{aligned}
D(\varrho_A||\sigma_A) &= \langle \varrho_A^{1/2}, -\log(\Delta_A)(\varrho_A^{1/2})\rangle_{HS} \\
&= \langle \varrho_A^{1/2}, -\log(U^*\Delta_{AB}U)(\varrho_A^{1/2})\rangle_{HS} \\
&\leq \langle \varrho_A^{1/2}, -U^*\log(\Delta_{AB})U(\varrho_A^{1/2})\rangle_{HS} \\
&= \langle U(\varrho_A^{1/2}), -\log(\Delta_{AB})(U(\varrho_A^{1/2}))\rangle_{HS} \\
&= \langle \varrho_{AB}^{1/2}, -\log(\Delta_{AB})(\varrho_{AB}^{1/2})\rangle_{HS} \\
&= D(\varrho_{AB}||\sigma_{AB})
\end{aligned} \tag{5.43}$$

Az általános esethez elég azt meggondolni, hogy minden T csatorna előáll $T(\varrho) = \mathrm{Tr}_E\, U\varrho U^*$ módon, ahol $U : \mathcal{H} \to \mathcal{K} \otimes \mathcal{H}_E$ izometria, és ekkor

$$D(T(\varrho)||T(\sigma)) \leq D(U\varrho U^*||U\sigma U^*) = D(\varrho||\sigma) \tag{5.44}$$

□

5.23. Következmény. *Ha $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $T_A : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_{A'})$ és $T_B : \mathcal{T}(\mathcal{H}_B) \to \mathcal{T}(\mathcal{H}_{B'})$ csatornák, akkor $I(A;B)_\varrho \geq I(A';B')_{(T_A\otimes T_B)(\varrho)}$.*

5.24. Következmény. *Ha $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $T : \mathcal{T}(\mathcal{H}_B) \to \mathcal{T}(\mathcal{H}_{B'})$ csatorna, akkor $H(A|B)_\varrho \leq H(A|B')_{(\mathrm{id}\otimes T)(\varrho)}$.*

5.25. Következmény. *Ha $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$, akkor $D(\varrho||\sigma) \geq 0$.*

5.26. Következmény. *Ha $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, akkor $I(A;B)_\varrho \geq 0$.*

5.27. Következmény. *Ha $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, akkor $|H(A|B)_\varrho| \leq \log\dim\mathcal{H}_A$.*

Bizonyítás. Legyen ϱ_{ABC} a ϱ_{AB} tiszta kiterjesztése, ekkor $H(A|B)_\varrho = -H(A|C)_\varrho$.

$$\log\dim\mathcal{H}_A - H(A|B)_\varrho = D\left(\varrho_{AB}||\frac{\mathrm{id}_{\mathcal{H}_A}}{\dim\mathcal{H}_A} \otimes \varrho_B\right) \geq 0 \tag{5.45}$$

azaz $H(A|B)_\varrho \leq \log\dim\mathcal{H}_A$ és hasonlóan $H(A|C)_\varrho \leq \log\dim\mathcal{H}_A$ □

5.28. Következmény. *Ha $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B)$, akkor $I(A;B))_\varrho \leq 2\log\min\{\dim\mathcal{H}_A, \dim\mathcal{H}_B\}$.*

Bizonyítás.

$$I(A;B)_\varrho = H(A)_\varrho - H(A|B)_\varrho \leq 2 \dim \mathcal{H}_A \tag{5.46}$$
$$I(A;B)_\varrho = H(B)_\varrho - H(B|A)_\varrho \leq 2 \dim \mathcal{H}_B \tag{5.47}$$

□

5.29. Példa. Legyen $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^d$, $|1\rangle, \ldots, |d\rangle$ a standard ortonormált bázis,

$$\varrho_{AB} = \sum_{i,i'=1}^{d} |i\rangle\langle i'| \otimes |i\rangle\langle i'| \tag{5.48}$$

Ekkor $H(A)_\varrho = H(B)_\varrho = \log d$, $H(AB)_\varrho = 0$, $H(A|B)_\varrho = -\log d$ és $I(A;B)_\varrho = 2\log d$

14. HF. Legyen $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^d$, $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ szeparált. Ekkor $I(A;B)_\varrho \leq \log d$.

5.30. Következmény. *Ha $\varrho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, akkor $I(A;B|C)_\varrho \geq 0$.*

Bizonyítás. $I(A;B|C)_\varrho = I(A;BC)_\varrho - I(A;B)_\varrho$ és

$$\begin{aligned} I(A;BC)_\varrho &= D(\varrho_{ABC}||\varrho_A \otimes \varrho_{BC}) \\ &\geq D(\varrho_{AB}||\varrho_A \otimes \varrho_B) \\ &= I(A;B)_\varrho \end{aligned} \tag{5.49}$$

□

5.31. Tétel (Erős szubadditivitás)**.** *Ha $\varrho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, akkor*

$$H(ABC)_\varrho + H(B)_\varrho \leq H(AB)_\varrho + H(BC)_\varrho \tag{5.50}$$

Bizonyítás.

$$\begin{aligned} 0 &\leq I(A;B|C)_\varrho \\ &= H(A|C) + H(B|C) - H(AB|C) \\ &= H(AC) - H(C) + H(BC) - H(C) - H(ABC) + H(C) \\ &= H(AC) + H(BC) - H(ABC) - H(C) \end{aligned} \tag{5.51}$$

□

5.32. Következmény. *Ha $\varrho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, akkor*

$$H(A|B)_\varrho \geq H(A|BC)_\varrho \tag{5.52}$$

Bizonyítás.

$$H(A|B)_\varrho - H(A|BC)_\varrho = H(AB)_\varrho - H(B)_\varrho - H(ABC)_\varrho + H(BC)_\varrho \quad (5.53)$$

□

5.33. Következmény. *Ha* $\varrho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, *akkor* $H(A)_\varrho \geq H(A|B)_\varrho$.

5.34. Következmény. *Ha* $\varrho \in \mathcal{S}(\mathcal{H})$, *akkor* $H(\varrho) \geq 0$. *Ha* $H(\varrho) = 0$, *akkor* ϱ *tiszta.*

5.35. Állítás (Együttes konvexitás)**.** *D a változóiban együttesen konvex, azaz ha* $P : \mathcal{X} \to [0,1]$ *valószínűségi eloszlás,* $\varrho_x, \sigma_x \in \mathcal{S}(\mathcal{H})$ $(\forall x \in \mathcal{X})$, *akkor*

$$D\left(\sum_{x\in\mathcal{X}} P(x)\varrho_x || \sum_{x\in\mathcal{X}} P(x)\sigma_x\right) \leq \sum_{x\in\mathcal{X}} P(x) D(\varrho_x||\sigma_x) \quad (5.54)$$

Bizonyítás. Legyen $\varrho = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \varrho_x \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H})$ és $\sigma = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \sigma_x$. Ekkor

$$\begin{aligned} D\left(\sum_{x\in\mathcal{X}} P(x)\varrho_x || \sum_{x\in\mathcal{X}} P(x)\sigma_x\right) &= D(\operatorname{Tr}_X \varrho || \operatorname{Tr}_X \sigma) \leq D(\varrho||\sigma) \\ &= \underbrace{D(P||P)}_{0} + \sum_{x\in\mathcal{X}} P(x) D(\varrho_x||\sigma_x) \end{aligned} \quad (5.55)$$

□

5.36. Következmény. $\varrho \mapsto H(A|B)_\varrho$ *konkáv.*

5.37. Következmény. $\varrho \mapsto H(A)_\varrho$ *konkáv.*

5.38. Tétel (Pinsker-egyenlőtlenség)**.** *Legyen* $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$. *Ekkor*

$$\frac{1}{2\ln 2}(\|\varrho - \sigma\|_1)^2 \leq D(\varrho||\sigma) \quad (5.56)$$

Bizonyítás. Először klasszikus kétállapotú rendszerekre bizonyítjuk. Legyen $\varrho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ és $\sigma = q|0\rangle\langle 0| + (1-q)|1\rangle\langle 1|$, feltehető, hogy $p \geq q$. Ekkor $\|\varrho - \sigma\|_1 = 2(p-q)$ és

$$D(\varrho||\sigma) = p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q} \quad (5.57)$$

Legyen

$$g(p,q) = p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q} - \frac{4}{2\ln 2}(p-q)^2 \quad (5.58)$$

q szerint deriválva:

$$\begin{aligned}\frac{\partial g(p,q)}{\partial q} &= -\frac{p}{q\ln 2} + \frac{1-p}{(1-q)\ln 2} - \frac{4}{\ln 2}(q-p)\\ &= -\frac{p(1-q)}{q(1-q)\ln 2} + \frac{q(1-p)}{q(1-q)\ln 2} - \frac{4}{\ln 2}(q-p)\\ &= \frac{q-p}{q(1-q)\ln 2} - \frac{4}{\ln 2}(q-p)\\ &= \frac{(q-p)(4q^2-4q+1)}{q(1-q)\ln 2}\\ &= \frac{(q-p)(2q-1)^2}{q(1-q)\ln 2} \le 0\end{aligned} \tag{5.59}$$

mivel $q \le p$. Tehát $g(p,q)$ akkor minimális $g \le p$ mellett, ha $q = p$, de ekkor $g(p,q) = 0$, tehát $g(p,q) \ge 0$.

Most legyen $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$ tetszőleges, $0 \le P \le 1$ olyan, hogy $\frac{1}{2}\|\varrho - \sigma\|_1 = |\operatorname{Tr}\varrho P - \operatorname{Tr}\sigma P|$. Tekintsük a $T : \mathcal{T}(\mathcal{H}) \to \ell^1(\{0,1\})$, $T(\varrho) = (\operatorname{Tr}\varrho P)|0\rangle\langle 0| + (\operatorname{Tr}\varrho(I-P))|1\rangle\langle 1|$ csatornát. Ekkor

$$\begin{aligned}D(\varrho||\sigma) &\ge D(T(\varrho)||T(\sigma))\\ &\ge \frac{1}{2\ln 2}\|T(\varrho) - T(\sigma)\|_1\\ &= \frac{1}{2\ln 2}2|\operatorname{Tr}\varrho P - \operatorname{Tr}\sigma P|\\ &= \frac{1}{2\ln 2}\|\varrho - \sigma\|_1\end{aligned} \tag{5.60}$$

□

5.39. Tétel (Alicki-Fannes-egyenlőtlenség)**.** *Legyen $\varrho_{AB}, \sigma_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Ekkor*

$$|H(A|B)_\varrho - H(A|B)_\sigma| \le 4\|\varrho_{AB} - \sigma_{AB}\|_1 \log\dim\mathcal{H}_A + 2h(\|\varrho_{AB} - \sigma_{AB}\|_1) \tag{5.61}$$

ahol $h(x) = -x\log x - (1-x)\log(1-x)$.

Bizonyítás. Legyen $\tilde{\varrho} = \frac{1}{\varepsilon}|\varrho - \sigma|$ és $\tilde{\varrho} = \frac{1-\varepsilon}{\varepsilon}(\varrho - \sigma) + \tilde{\varrho}$, ezek állapotok. Tekintsük a

$$\gamma_{XAB} = (1-\varepsilon)|0\rangle\langle 0| \otimes \varrho + \varepsilon|1\rangle\langle 1| \otimes \tilde{\varrho} \tag{5.62}$$

klasszikus-kvantum-kvantum állapotot. Erre

$$\gamma_{AB} = \operatorname{Tr}_X \gamma_{XAB} = (1-\varepsilon)\varrho + \varepsilon\tilde{\varrho} = (1-\varepsilon)\sigma + \varepsilon\tilde{\sigma} \tag{5.63}$$

teljesül. Mivel a feltételes entrópia konkáv, $H(A|B)_\gamma \ge (1-\varepsilon)H(A|B)_\varrho + \varepsilon H(A|B)_{\tilde{\varrho}}$. Emiatt

$$\begin{aligned}H(A|B)_\varrho - H(A|B)_\gamma &\le \varepsilon\left(H(A|B)_\varrho - H(A|B)_{\tilde{\varrho}}\right)\\ &\le 2\varepsilon\log\dim\mathcal{H}_A\\ &\le 2\varepsilon\log\dim\mathcal{H}_A + h(\varepsilon)\end{aligned} \tag{5.64}$$

Másfelől az entrópia konkavitása miatt

$$H(B)_\gamma \geq (1-\varepsilon)H(B)_\varrho + \varepsilon H(B)_{\tilde{\varrho}} \tag{5.65}$$

Továbbá $0 \leq H(AB|X) = H(ABX)_\gamma - H(AB)_\gamma$. Emiatt

$$\begin{aligned} H(AB)_\gamma &\leq H(AB|X)_\gamma + H(X)_\gamma \\ &= (1-\varepsilon)H(AB)_\varrho + \varepsilon H(AB)_{\tilde{\varrho}} + h(\varepsilon) \end{aligned} \tag{5.66}$$

amit az előző egyenlőtlenséggel kombinálva

$$\begin{aligned} H(A|B)_\gamma - H(A|B)_\varrho \leq &(1-\varepsilon)H(A|B)_\varrho + \varepsilon H(A|B)_{\tilde{\varrho}} \\ &+ h(\varepsilon) - H(A|B)_\varrho \\ =&\varepsilon\left(H(A|B)_{\tilde{\varrho}} - H(A|B)_\varrho\right) + h(\varepsilon) \\ \leq &2\varepsilon \log \dim \mathcal{H}_A + h(\varepsilon) \end{aligned} \tag{5.67}$$

adódik.

Ugyanígy kapjuk, hogy

$$|H(A|B)_\sigma - H(A|B)_\gamma| \leq 2\varepsilon \log \dim \mathcal{H}_A + h(\varepsilon) \tag{5.68}$$

és így a háromszög-egyenlőtlenség miatt

$$|H(A|B)_\varrho - H(A|B)_\sigma| \leq 4\varepsilon \log \dim \mathcal{H}_A + 2h(\varepsilon) \tag{5.69}$$

$\square$

5.40. Definíció. Egy $\varrho \in \mathcal{S}(\mathcal{H})$ állapot Rényi-entrópiája

$$H_\alpha(\varrho) = \frac{1}{1-\alpha} \log \operatorname{Tr} \varrho^\alpha \tag{5.70}$$

- $H_0(\varrho) := \lim_{\alpha\to 0} H_\alpha(\varrho) = \log \dim \operatorname{supp} \varrho$
- $H_\infty(\varrho) := \lim_{\alpha\to\infty} H_\alpha(\varrho) = -\log \|\varrho\|_\infty$
- $\lim_{\alpha\to 1} H_\alpha(\varrho) = -\operatorname{Tr} \varrho \log \varrho$ a Neumann-entrópia
- $0 \leq \alpha \leq \beta \leq \infty$ esetén $H_\alpha(\varrho) \geq H_\beta(\varrho)$

5.41. Definíció. Egy $\varrho \in \mathcal{S}(\mathcal{H})$ állapot sima Rényi-entrópiája $0 < \varepsilon < 1$ esetén

$$H_\alpha^\varepsilon(\varrho) = \inf_{\sigma\in B_\varepsilon(\varrho)} H_\alpha(\sigma) \tag{5.71}$$

ha $0 \leq \alpha < 1$ és

$$H_\alpha^\varepsilon(\varrho) = \sup_{\sigma\in B_\varepsilon(\varrho)} H_\alpha(\sigma) \tag{5.72}$$

ha $1 < \alpha \leq \infty$, ahol $B_\varepsilon(\varrho) = \{\sigma \in \mathcal{S}(\mathcal{H}) | \frac{1}{2}\|\sigma - \varrho\|_1 < \varepsilon\}$.

5.42. Tétel (Aszimptotikus ekvipartíció tulajdonság)**.** *Legyen* $\varrho \in \mathcal{S}(\mathcal{H})$*. Ekkor*

$$\lim_{\varepsilon\to 0}\limsup_{n\to\infty}\frac{1}{n}H_0^\varepsilon(\varrho^{\otimes n}) = \lim_{\varepsilon\to 0}\liminf_{n\to\infty}\frac{1}{n}H_0^\varepsilon(\varrho^{\otimes n}) = H(\varrho) \tag{5.73}$$

Bizonyítás. Legyen $\varrho = \sum_{i\in I} p_i|i\rangle\langle i|$, ahol $(|i\rangle)_{i\in I}$ ortonormáltak, $(p_i)_{i\in I}$ valószínűségi eloszlás. Ekkor

$$\varrho^{\otimes n} = \sum_{i_1\dots i_n\in I^n} p_{i_1}\dots p_{i_n}|i_1\dots i_n\rangle\langle i_1\dots i_n| \tag{5.74}$$

Legyen $\delta > 0$ rögzített,

$$A_\delta^{(n)} = \{(i_1\dots i_n)\in I^n | 2^{-n(H(\varrho)+\delta)} \le p_{i_1}\dots p_{i_n} \le 2^{-n(H(\varrho)-\delta)}\} \tag{5.75}$$

és

$$\Pi_\delta^{(n)} = \sum_{i_1\dots i_n\in A_\delta^{(n)}} |i_1\dots i_n\rangle\langle i_1\dots i_n| \tag{5.76}$$

Ekkor a nagy számok gyenge törvénye miatt
$\lim_{n\to\infty}\operatorname{Tr}\Pi_\delta^{(n)}\varrho^{\otimes n} = 1$. Másrészt

$$1 = \sum_{i_1\dots i_n} p_{i_1}\dots p_{i_n} \ge |A_\delta^{(n)}|2^{-n(H(\varrho)+\delta)} \tag{5.77}$$

Tehát

$$\left\|\varrho - \frac{\Pi_\delta^{(n)}\varrho\Pi_\delta^{(n)}}{\operatorname{Tr}\Pi_\delta^{(n)}\varrho\Pi_\delta^{(n)}}\right\|_1 = 2\left\|\varrho - \Pi_\delta^{(n)}\varrho\Pi_\delta^{(n)}\right\|_1 = 2(1-\operatorname{Tr}\Pi_\delta^{(n)}\varrho) \to 0 \tag{5.78}$$

és így minden $\varepsilon,\delta > 0$ mellett elég nagy n-re

$$H_0^\varepsilon(\varrho^{\otimes n}) \le H_0\left(\frac{\Pi_\delta^{(n)}\varrho\Pi_\delta^{(n)}}{\operatorname{Tr}\Pi_\delta^{(n)}\varrho\Pi_\delta^{(n)}}\right) \le \log\operatorname{rk}\Pi_\delta^{(n)} = \log|A_\delta^{(n)}| \le n(H(\varrho)+\delta) \tag{5.79}$$

amiből $\varepsilon > 0$ esetén

$$\limsup_{n\to\infty}\frac{1}{n}H_0^\varepsilon(\varrho^{\otimes n}) \le H(\varrho) \tag{5.80}$$

A másik irányhoz az Alicki-Fannes-egyenlőtlenséget használhatjuk:

$$\begin{aligned}\liminf_{n\to\infty}\frac{1}{n}H_0^\varepsilon(\varrho^{\otimes n}) =&\liminf_{n\to\infty}\frac{1}{n}\inf_{\sigma\in B_\varepsilon(\varrho^{\otimes n})}H_0(\sigma)\\ \ge&\liminf_{n\to\infty}\frac{1}{n}\inf_{\sigma\in B_\varepsilon(\varrho^{\otimes n})}H(\sigma)\\ \ge&\liminf_{n\to\infty}\frac{1}{n}\inf_{\sigma\in B_\varepsilon(\varrho^{\otimes n})}(H(\varrho^{\otimes n})\\ &-2\varepsilon n\log\dim\mathcal{H}-2)\\ =&H(\varrho)-2\varepsilon\end{aligned} \tag{5.81}$$

□

15. HF. Legyen $\varrho \in \mathcal{S}(\mathcal{H})$. Ekkor

$$\lim_{\varepsilon\to 0}\limsup_{n\to\infty}\frac{1}{n}H_\infty^\varepsilon(\varrho^{\otimes n}) = \lim_{\varepsilon\to 0}\liminf_{n\to\infty}\frac{1}{n}H_\infty^\varepsilon(\varrho^{\otimes n}) = H(\varrho) \tag{5.82}$$

6. Forráskódolás

- adott $\varrho_{RA} \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_A)$ állapot, ennek „A” felét szeretnénk egy (pl. térben távoli) „B” helyre továbbítani
- rendelkezésre áll egy ideális qubit csatorna $qc : \mathcal{T}(\mathbb{C}^2) \to \mathcal{T}(\mathbb{C}^2)$, $qc(\varrho) = \varrho$
- lokálisan bármilyen transzformációt ingyen végezhetünk
- hányszor kell használni a csatornát?
- tegyük fel, hogy az „R” részt nem ismerjük, ekkor feltehető, hogy ϱ_{RA} a ϱ_A tiszta kiterjesztése, mert a tényleges ϱ_{RA} ebből esetleges parciális trace segítségével megkapható (ez a legrosszabb eset)

6.1. Definíció. Legyen $\varrho_A \in \mathcal{S}(\mathcal{H}_A)$, $\varepsilon > 0$ és $m \in \mathbb{N}$. Egy (E, D) pár a ϱ_A állapot m qubites ε-kódolása, ha $E : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}((\mathcal{C}^2)^{\otimes m})$, $D : \mathcal{T}((\mathcal{C}^2)^{\otimes m}) \to \mathcal{T}(\mathcal{H}_A)$ csatornák és

$$\left\| \varrho_{RA} - (\mathrm{id}_{\mathcal{T}(\mathcal{H}_R)} \otimes (D \circ E))\varrho_{RA}) \right\|_1 \leq \varepsilon \tag{6.1}$$

ahol ϱ_{RA} a ϱ_A tiszta kiterjesztése.

6.2. Állítás. *Legyen $\varrho_A \in \mathcal{S}(\mathcal{H}_A)$ és $\varepsilon \in (0,1)$. Ekkor létezik ϱ_A-nak $m = \lceil H_0^\varepsilon(\varrho_A) \rceil$ qubites $\sqrt{8\varepsilon}$-kódolása.*

Bizonyítás. Legyen $\sigma \in \mathcal{S}(\mathcal{H}_A)$ olyan, hogy $H_0(\sigma) = H_0^\varepsilon(\varrho_A)$ és $\frac{1}{2}\left\|\sigma - \varrho_A\right\|_1 \leq \varepsilon$. Legyen P a $\operatorname{supp}\sigma$ projektora. Ekkor

$$\begin{aligned} \mathrm{Tr}(I_R \otimes P)\varrho_{RA} &= \mathrm{Tr}\, P\varrho_A \\ &= \mathrm{Tr}\, P\sigma - \mathrm{Tr}\, P(\sigma - \varrho_A) \\ &\geq \mathrm{Tr}\, P\sigma - \frac{1}{2}\left\|\sigma - \varrho_A\right\|_1 \\ &\geq 1 - \varepsilon \end{aligned} \tag{6.2}$$

Legyen $T_1 : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_A \otimes \mathbb{C}^2)$ a $T_1(\varrho) = P\varrho P \otimes |0\rangle\langle 0| + (I-P)\varrho(I-P)|1\rangle\langle 1|$ képlettel adott csatorna. Ekkor

$$\begin{aligned} (\mathrm{id}_{\mathcal{T}(\mathcal{H}_R)} \otimes T_1)(\varrho) = (I_R \otimes P)\varrho(I_R \otimes P) \otimes |0\rangle\langle 0| \\ + (I_R \otimes (I-P))\varrho(I_R \otimes (I-P)) \otimes |1\rangle\langle 1| \end{aligned} \tag{6.3}$$

Gentle measurement miatt

$$\frac{1}{2}\left\| \varrho_{RA} \otimes |0\rangle\langle 0| - (\mathrm{id}_{\mathcal{T}(\mathcal{H}_R)} \otimes T_1)(\varrho_{RA}) \right\|_1 \leq 2\sqrt{\varepsilon} \tag{6.4}$$

Legyen $T_2 : \mathcal{T}(\mathcal{H}_A \otimes \mathbb{C}^2) \to \mathcal{T}(\mathcal{H}_A)$ a $T(\varrho \otimes \gamma) = \varrho \langle 0|\gamma|0\rangle + \frac{P}{\operatorname{Tr} P}(\operatorname{Tr} \varrho)\langle 1|\gamma|1\rangle$ képlettel adva, ekkor bármely állapot $T_2 \circ T_1$ általi képének tartója $\operatorname{supp} \sigma$ része.

Legyen $U : \mathcal{H}_A \to (\mathbb{C}^2)^{\otimes m}$ parciális izometria, ami $\operatorname{supp} \sigma$-n izometria és legyen $T_3 : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}((\mathbb{C}^2)^{\otimes m})$ a $T(\varrho) = U \varrho U^*$ leképezés. Ez nem csatorna, de $E := T_3 \circ T_2 \circ T_1$ igen.

Legyen $D : \mathcal{T}((\mathbb{C}^2)^{\otimes m}) \to \mathcal{T}(\mathcal{H}_A)$ a

$$D(\varrho) = U^* \varrho U + \operatorname{Tr}((I - UU^*)\varrho) \frac{I_A}{\dim \mathcal{H}_A} \tag{6.5}$$

csatorna.

Ekkor $D \circ E = T_2 \circ T_1$ és $T_2(\varrho_{RA} \otimes |0\rangle\langle 0|) = \varrho_{RA}$ alapján

$$\left\| \varrho_{RA} - (\mathrm{id}_{\mathcal{T}(\mathcal{H}_R)} \otimes (D \circ E))(\varrho_{RA}) \right\|_1 \leq \sqrt{8\varepsilon} \tag{6.6}$$

□

6.3. Állítás. *Legyen $\varrho_A \in \mathcal{S}(\mathcal{H}_A)$, $\varepsilon \in (0,1)$, $m \in \mathbb{N}$ és tegyük fel, hogy létezik ϱ_A-nak m qubites ε-kódolása. Ekkor*

$$m \geq H(\varrho_A) - 4\varepsilon \log \dim \mathcal{H}_A - h(\varepsilon) \tag{6.7}$$

Bizonyítás. Legyen (E, D) a ϱ_A egy m qubites ε-kódolása. Ekkor az Alicki-Fannes-egyenlőtlenség és az adatfeldolgozási egyenlőtlenség alapján

$$\begin{aligned} 2H(\varrho_A) &= I(R;A)_\varrho \\ &\leq I(R;A)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_R)} \otimes (D \circ E))\varrho} + 8\varepsilon \log \dim \mathcal{H}_A + 2h(\varepsilon) \\ &\leq I(R;A)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_R)} \otimes E)\varrho} + 8\varepsilon \log \dim \mathcal{H}_A + 2h(\varepsilon) \\ &\leq 2m + 8\varepsilon \log \dim \mathcal{H}_A + 2h(\varepsilon) \end{aligned} \tag{6.8}$$

□

- forrás: referencia-rendszerrel korrelált állapotokat állít elő „A" rendszeren
- cél: forrás és $A \to B$ qubit csatorna segítségével az állapotokat a „B" rendszerbe átvinni, miközben a referencia-rendszerrel való korreláció megmarad (kis hibától eltekintve)

6.4. Definíció. Legyenek $\mathcal{H}_{A_1}, \mathcal{H}_{A_2}, \mathcal{H}_{A_3}, \ldots$ Hilbert-terek. Egy $\varrho = (\varrho_{A_1}, \varrho_{A_1 A_2}, \ldots)$ sorozat (kvantum) forrás, ha minden $n \in \mathbb{N}$-re $\varrho_{A_1 \ldots A_n} \in \mathcal{S}(\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_n})$ és $\varrho_{A_1 \ldots A_n} = \operatorname{Tr}_{A_{n+1}} \varrho_{A_1 \ldots A_{n+1}}$.

- pl.: Legyen $\mathcal{H}_{A_i} = \mathcal{H}$, $\varrho_0 \in \mathcal{S}(\mathcal{H})$. Ekkor a $\varrho = (\varrho_0, \varrho_0^{\otimes 2}, \varrho_0^{\otimes 3}, \ldots)$ sorozat a ϱ_0 eloszlásnak megfelelő FAE (IID) forrás.

6.5. Definíció. Legyen $\varrho_{A_1}, \dots$ forrás. Egy $(m_n, \varepsilon_n, E_n, D_n)_{n\in\mathbb{N}}$ sorozat (aszimptotikusan hibamentes) (forrás)kódolás, ha (E_n, D_n) a $\varrho_{A_1\dots A_n}$ egy m_n qubites ε_n-kódolása és

$$\lim_{n\to\infty} \varepsilon_n = 0 \tag{6.9}$$

- cél: adott forráshoz olyan $(m_n, \varepsilon_n, E_n, D_n)_{n\in\mathbb{N}}$ kódolást keresni, amire

$$\limsup_{n\to\infty} \frac{m_n}{n} \tag{6.10}$$

  a lehető legkisebb.

6.6. Állítás.

$$\min\left\{ \limsup_{n\to\infty} \frac{m_n}{n} \middle| (m_n, \varepsilon_n, E_n, D_n)_{n\in\mathbb{N}} \textit{ a } \varrho \textit{ aszimptotikusan hibamentes kódolása} \right\}$$
$$= \lim_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \min\{m \in \mathbb{N} | \exists \varrho_{A_1\dots A_n}\textit{-nek } m \textit{ qubites } \varepsilon\textit{-kódolása}\} \tag{6.11}$$

ahol a

Bizonyítás. A jobb oldalon ε monoton csökkenő függvényének vesszük limeszét, tehát az létezik.

Legyen $(m_n, \varepsilon_n, E_n, D_n)_{n\in\mathbb{N}}$ a ϱ aszimptotikusan hibamentes kódolása, $R = \limsup_{n\to\infty} \frac{m_n}{n}$. Ekkor tetszőleges $\varepsilon > 0$-ra és elég nagy n-re $\varepsilon_n < \varepsilon$, tehát

$$\min\{m \in \mathbb{N} | \exists \varrho_{A_1\dots A_n}\text{-nek } m \text{ qubites } \varepsilon\text{-kódolása}\} \le m_n \tag{6.12}$$

amiből

$$\lim_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \min\{m \in \mathbb{N} | \exists \varrho_{A_1\dots A_n}\text{-nek } m \text{ qubites } \varepsilon\text{-kódolása}\}$$
$$\le \lim_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{m_n}{n} = R \tag{6.13}$$

Most legyen R a jobb oldal. Bármely $\varepsilon > 0$-hoz létezik olyan $n_0(\varepsilon)$, hogy $n \ge n_0(\varepsilon)$ esetén

$$\min\{m \in \mathbb{N} | \exists \varrho_{A_1\dots A_n}\text{-nek } m \text{ qubites } \varepsilon\text{-kódolása}\} \le (R+\varepsilon)n \tag{6.14}$$

Válasszunk tetszőleges ε_k pozitív tagú csökkenő nullsorozatot, és legyen $n_0(\varepsilon_k)$-tól kezdve (E_n, D_n) egy m_n-qubites ε_k-kódolás, ahol $m_n \le (R+\varepsilon)n$. Ekkor $(m_n, \varepsilon_n, E_n, D_n)_{n\in\mathbb{N}}$ a ϱ aszimptotikusan hibamentes kódolása és

$$\limsup_{n\to\infty} \frac{m_n}{n} = R \tag{6.15}$$

$\square$

6.7. Tétel (Schumacher-tömörítés). *Legyen $\varrho_0 \in \mathcal{S}(\mathcal{H})$, $\varrho = (\varrho_0, \varrho_0^{\otimes 2}, \varrho_0^{\otimes 3}, \dots)$ a ϱ_0 eloszlásnak megfelelő IID forrás. Ekkor pontosan akkor létezik ϱ-nak olyan $(m_n, \varepsilon_n, E_n, D_n)_{n\in\mathbb{N}}$ aszimptotikusan hibamentes kódolása, amire*

$$\limsup_{n\to\infty} \frac{m_n}{n} = R \tag{6.16}$$

ha $R \geq H(\varrho_0)$.

Bizonyítás.

$$\begin{aligned}\limsup_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \min\{m \in \mathbb{N} | \exists \varrho_0^{\otimes n}\text{-nek } m \text{ qubites } \varepsilon\text{-kódolása}\} \\ \leq \limsup_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \left\lceil H_0^{\varepsilon^2/8}(\varrho_0^{\otimes n}) \right\rceil = H(\varrho_0)\end{aligned} \tag{6.17}$$

$$\begin{aligned}\liminf_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \min\{m \in \mathbb{N} | \exists \varrho_0^{\otimes n}\text{-nek } m \text{ qubites } \varepsilon\text{-kódolása}\} \\ \geq \liminf_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} (H(\varrho_0^{\otimes n}) - 4\varepsilon \log \dim \mathcal{H}_A^{\otimes n} - h(\varepsilon)) \\ = \liminf_{\varepsilon\to 0} H(\varrho_0) - 4\varepsilon \log \dim \mathcal{H}_A = H(\varrho_0)\end{aligned} \tag{6.18}$$

□

7. Klasszikus kapacitás

- $cc : \ell^1(\{0,1\}) \to \ell^1(\{0,1\})$ ideális klasszikus bit csatorna
- $qc : \mathcal{T}(\mathbb{C}^2) \to \mathcal{T}(\mathbb{C}^2)$ ideális kvantum bit csatorna
- cél: (zajos) kvantum csatorna segítségével ezek tenzorhatványit „szimulálni”, vagyis információt továbbítani aszimptotikusan eltűnő hibával

7.1. Definíció. Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna, $\varepsilon > 0$ és $m \in \mathbb{N}$. Egy (E, D) pár a T-hez tartozó m bit ε-csatornakódolás, ha $E : \ell^1(\{0,1\})^{\otimes m} \to \mathcal{T}(\mathcal{H}_A)$, $D : \mathcal{T}(\mathcal{H}_B) \to \ell^1(\{0,1\})^{\otimes m}$ csatornák és

$$\left\| D \circ T \circ E - cc^{\otimes m} \right\|_{1-1} \leq \varepsilon \tag{7.1}$$

7.2. Definíció. A $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna klasszikus kapacitása

$$\begin{aligned}C(T) = \lim_{\varepsilon\to 0} \liminf_{n\to\infty} \frac{1}{n} \max\{m \in \mathbb{N} | \exists E : \ell^1(\{0,1\})^{\otimes m} \to \mathcal{T}(\mathcal{H}_A^{\otimes n}), \\ D : \mathcal{T}(\mathcal{H}_B^{\otimes n}) \to \ell^1(\{0,1\})^{\otimes m} : \left\| D \circ T^{\otimes n} \circ E - cc^{\otimes m} \right\|_{1-1} < \varepsilon\}\end{aligned} \tag{7.2}$$

16. HF. Legyen $T : \ell^1(\mathcal{X}) \to \ell^1(\mathcal{Y})$ lineáris leképezés. Ekkor $\|T\|_{1-1} = \|T\|_\diamondsuit$.

7.3. Definíció. Egy $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna Holevo-információja

$$\chi(T) = \sup_{\varrho_{XA}} I(X;B)_{\mathrm{id}_{\ell^1(\mathcal{X})} \otimes T(\varrho)} \tag{7.3}$$

ahol a szuprémum tetszőleges $\varrho_{XA} \in \ell^1(\mathcal{X}) \otimes \mathcal{T}(\mathcal{H}_A)$ klasszikus-kvantum állapotokon értendő.

7.4. Tétel. *Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna és tegyük fel, hogy $0 < \varepsilon < \frac{1}{8}$ és (E, D) egy T-hez tartozó m bit ε-csatornakódolás. Ekkor*

$$m \leq \frac{\chi(T) + 2h(\varepsilon)}{1 - 8\varepsilon} \tag{7.4}$$

Bizonyítás. Legyen (E, D) a T-hez tartozó m bit ε-csatornakódolás és tekintsük a

$$\Phi = \left(\frac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \otimes |1\rangle\langle 1|\right)^{\otimes m} \in \ell^1(\mathcal{X}) \otimes \ell^1(\mathcal{Y}) \tag{7.5}$$

állapotot, ahol $\mathcal{X} = \mathcal{Y} = \{0,1\}^m$. Erre $I(X;Y)_\Phi = m$, tehát az Alicki-Fannes-egyenlőtlenség és az adatfeldolgozási egyenlőtlenség alapján

$$\begin{aligned} m &= I(X;Y)_\Phi \\ &= I(X;Y)_{\mathrm{id}_{\ell^1(\mathcal{X})} \otimes cc^{\otimes m}(\Phi)} \\ &\leq I(X;Y)_{\mathrm{id}_{\ell^1(\mathcal{X})} \otimes D \circ T \circ E(\Phi)} + 8\varepsilon m + 2h(\varepsilon) \\ &\leq I(X;B)_{\mathrm{id}_{\ell^1(\mathcal{X})} \otimes T(\mathrm{id}_{\ell^1(\mathcal{X})} \otimes E(\Phi))} + 8\varepsilon m + 2h(\varepsilon) \\ &\leq \chi(T) + 8\varepsilon m + 2h(\varepsilon) \end{aligned} \tag{7.6}$$

□

7.5. Állítás. *A Holevo-információ szuperadditív, azaz ha $T_i : \mathcal{T}(\mathcal{H}_{A,i}) \to \mathcal{T}(\mathcal{H}_{B,i})$ csatornák ($i = 1, 2$), akkor $\chi(T_1 \otimes T_2) \geq \chi(T_1) + \chi(T_2)$.*

Bizonyítás. Legyen $\varrho_i \in \ell^1(\mathcal{X}_i) \otimes \mathcal{T}(\mathcal{H}_{A,i})$ olyan klasszikus-kvantum állapot, amire $I(X_i;B_i)_{(\mathrm{id}_{\ell^1(\mathcal{X}_i)} \otimes T_i)(\varrho_i)} = \chi(T_i)$. Ekkor

$$\begin{aligned} \chi(T_1 \otimes T_2) = &\sup_{\varrho_{XA_1A_2}} I(X;B_1B_2)_{\mathrm{id}_{\ell^1(\mathcal{X})} \otimes T_1 \otimes T_2(\varrho)} \\ &\geq I(X_1X_2;B_1B_2)_{(\mathrm{id}_{\ell^1(\mathcal{X}_1)} \otimes T_1)(\varrho_1) \otimes (\mathrm{id}_{\ell^1(\mathcal{X}_2)} \otimes T_2)(\varrho_2)} \\ &= I(X_1;B_1)_{(\mathrm{id}_{\ell^1(\mathcal{X}_1)} \otimes T_1)(\varrho_1)} \\ &\quad + I(X_2;B_2)_{(\mathrm{id}_{\ell^1(\mathcal{X}_2)} \otimes T_2)(\varrho_2)} \\ &= \chi(T_1) + \chi(T_2) \end{aligned} \tag{7.7}$$

□

7.6. Következmény. *Tetszőleges $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna esetén létezik a*

$$\chi_{reg}(T) := \lim_{k\to\infty} \frac{1}{k}\chi(T^{\otimes k}) \tag{7.8}$$

limesz.

7.7. Következmény. *Tetszőleges $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna esetén $C(T) \leq \chi_{reg}(T)$.*

7.8. Lemma (Hayashi-Nagaoka-egyenlőtlenség)**.** *Legyenek S, T pozitív operátorok, $S \leq I$. Ekkor*

$$I - (S+T)^{-1/2}S(S+T)^{-1/2} \leq 2(I-S) + 4T \tag{7.9}$$

ahol az inverz a tartón értendő.

Bizonyítás. Először tegyük fel, hogy $S+T$ invertálható. Tetszőleges A, B operátorokra $0 \leq (A-B)^*(A-B) = A^*A + B^*B - (A^*B + B^*A)$ teljesül. $A = \sqrt{T}$, $B = \sqrt{T}(\sqrt{S+T}^{-1} - I)$ választással

$$T(\sqrt{S+T}^{-1} - I) + (\sqrt{S+T}^{-1} - I)T \leq T + (\sqrt{S+T}^{-1} - I)T(\sqrt{S+T}^{-1} - I) \tag{7.10}$$

Mivel $x \mapsto \sqrt{x}$ operátormonoton és $0 \leq S \leq I$, $S \leq \sqrt{S} \leq \sqrt{S+T}$. Ezek felhasználásával:

$$\begin{aligned}
&I - \sqrt{S+T}^{-1}S\sqrt{S+T}^{-1} \\
&= \sqrt{S+T}^{-1}T\sqrt{S+T}^{-1} \\
&= T + T(\sqrt{S+T}^{-1} - I) + (\sqrt{S+T}^{-1} - I)T + (\sqrt{S+T}^{-1} - I)T(\sqrt{S+T}^{-1} - I) \\
&\leq 2T + 2(\sqrt{S+T}^{-1} - I)T(\sqrt{S+T}^{-1} - I) \\
&\leq 2T + 2(\sqrt{S+T}^{-1} - I)(S+T)(\sqrt{S+T}^{-1} - I) \\
&= 2T + 2(I + S + T - 2\sqrt{S+T}) \\
&\leq 2T + 2(I + S + T - 2S) = 2(I-S) + 4T
\end{aligned} \tag{7.11}$$

Az általános legyen P az $S+T$ tartójának projektora, ekkor a fenti egyenlőtlenség teljesül I helyére P-t írva. Ehhez pedig csak hozzá kell adni az $I - P \leq 2(I-P)$ egyenlőtlenséget. □

7.9. Lemma (Pakolási lemma)**.** *Legyen $\mathcal{X}$ véges halmaz, $P_X : \mathcal{X} \to [0,1]$ diszkrét eloszlás, $\sigma_x \in \mathcal{S}(\mathcal{H})$ állapotok ($\forall x \in \mathcal{X}$), $\sigma = \sum_{x\in\mathcal{X}} P_X(x)\sigma_x$. Legyenek továbbá $\Pi, \Pi_x \in \mathcal{B}(\mathcal{H})$ projektrok ($\forall x \in \mathcal{X}$) és tegyük fel, hogy* *az alábbiak teljesülnek:*

$$\begin{aligned}
\operatorname{Tr}\sigma_x\Pi &\geq 1-\varepsilon && (7.12)\\
\operatorname{Tr}\sigma_x\Pi_x &\geq 1-\varepsilon && (7.13)\\
\operatorname{Tr}\Pi_x &\leq d && (7.14)\\
\Pi\sigma\Pi &\leq \frac{1}{D}\Pi && (7.15)\\
& && (7.16)
\end{aligned}$$

ahol $0 < d < D$, $0 < \varepsilon < 1$. *Ekkor bármely véges* $\mathcal{M}$ *halmazhoz létezik olyan* $c : \mathcal{M} \to \mathcal{X}$ *függvény és* $(\Lambda_m)_{m\in\mathcal{M}\sqcup\{e\}}$ *POVM, amire* $\forall m \in \mathcal{M}$ *esetén*

$$\operatorname{Tr}\sigma_{c_m}\Lambda_m \geq 1 - 4(\varepsilon + 2\sqrt{\varepsilon}) - 16\frac{d|\mathcal{M}|}{D} \tag{7.17}$$

teljesül.

Bizonyítás. Először legyen c véletlen függvény, c_m független azonos P_X eloszlással és legyen

$$\Lambda_m = \left(\sum_{m'\in\mathcal{M}} \Pi\Pi_{c_{m'}}\Pi\right)^{-\frac{1}{2}} \Pi\Pi_{c_m}\Pi \left(\sum_{m'\in\mathcal{M}} \Pi\Pi_{c_{m'}}\Pi\right)^{-\frac{1}{2}} \tag{7.18}$$

és $\Lambda_e = I - \sum_{m\in\mathcal{M}} \Lambda_m$.

Az előző lemmát használjuk

$$T = \sum_{m'\in\mathcal{M}\setminus\{m\}} \Pi\Pi_{c_{m'}}\Pi \qquad S = \Pi\Pi_{c_m}\Pi \tag{7.19}$$

szereposztással:

$$I - \Lambda_m \leq 2(I - \Pi\Pi_{c_m}\Pi) + 4 \sum_{m'\in\mathcal{M}\setminus\{m\}} \Pi\Pi_{c_{m'}}\Pi \tag{7.20}$$

Ezzel az m üzenet sikertelen azonosításának valószínűségére:

$$\operatorname{Tr}(I-\Lambda_m)\sigma_{c_m} \leq 2\operatorname{Tr}(I-\Pi\Pi_{c_m}\Pi)\sigma_{c_m} + 4 \sum_{m'\in\mathcal{M}\setminus\{m\}} \operatorname{Tr}\Pi\Pi_{c_{m'}}\Pi\sigma_{c_m} \tag{7.21}$$

Ezek m szerint átlagának várható értéket szeretnénk becsülni. Az első taghoz:

$$\begin{aligned}
\operatorname{Tr}\Pi\Pi_{c_m}\Pi\sigma_{c_m} &= \operatorname{Tr}\Pi_{c_m}\Pi\sigma_{c_m}\Pi \\
&\geq \operatorname{Tr}\Pi_{c_m}\sigma_{c_m} - \|\Pi\sigma_{c_m}\Pi - \sigma_{c_m}\|_1 \\
&\geq 1 - \varepsilon - 2\sqrt{\varepsilon}
\end{aligned} \tag{7.22}$$

a feltételek és a gentle measurement miatt, tehát $\operatorname{Tr}(I - \Pi\Pi_{c_m}\Pi)\sigma_{c_m} \leq \varepsilon + 2\sqrt{\varepsilon}$. A második tagból:

$$\mathbb{E}\,\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\operatorname{Tr}(I-\Lambda_m)\sigma_{c_m} \leq 2(\varepsilon+2\sqrt{\varepsilon}) + \frac{4}{|\mathcal{M}|}\sum_{\substack{m,m'\in\mathcal{M}\\ m\neq m'}}\mathbb{E}\operatorname{Tr}\Pi\Pi_{c_{m'}}\Pi\sigma_{c_m} \tag{7.23}$$

Itt a várható értékre a függetlenség miatt

$$\begin{aligned}\mathbb{E}\operatorname{Tr}\Pi\Pi_{c_{m'}}\Pi\sigma_{c_m} &= \operatorname{Tr}\Pi(\mathbb{E}\,\Pi_{c_{m'}})\Pi(\mathbb{E}\,\sigma_{c_m}) \\ &= \operatorname{Tr}(\mathbb{E}\,\Pi_{c_{m'}})\Pi(\sigma)\Pi \leq \operatorname{Tr}(\mathbb{E}\,\Pi_{c_{m'}})\frac{1}{D}\Pi \\ &\leq \frac{1}{D}\operatorname{Tr}(\mathbb{E}\,\Pi_{c_{m'}}) = \frac{1}{D}\,\mathbb{E}\operatorname{Tr}(\Pi_{c_{m'}}) \\ &\leq \frac{d}{D}\end{aligned} \tag{7.24}$$

amiből

$$\mathbb{E}\,\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\operatorname{Tr}\Lambda_m\sigma_{c_m} \geq 1 - 2(\varepsilon+2\sqrt{\varepsilon}) - 4\frac{d|\mathcal{M}|}{D} \tag{7.25}$$

Mivel a várható érték kisebb a maximumnál, létezik olyan $(c_m)_{m\in\mathcal{M}}$ választás, amivel ugyanez az alsó korlát érvényes (várható érték nélkül). Mivel minden tag legfeljebb 1, a tagok legfeljebb fele kisebb mint $1 - 4(\varepsilon+2\sqrt{\varepsilon}) - 8\frac{d|\mathcal{M}|}{D}$. Csak ezeket megtartva a kívánt tulajdonságú függvényt kapunk, de $\mathcal{M}$ helyett annak egy $|\mathcal{M}|/2$ elemű részhalmazával. Az állítás bizonyításához elég egy kétszer ekkora kiinduló halmazt használni. □

7.10. Tétel (Holevo-Schumacher-Westmoreland)**.** *Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna. Ekkor $C(T) \geq \chi(T)$.*

Bizonyítás. Legyen $\varrho_{XA} \in \ell^1(\mathcal{X}) \otimes \mathcal{T}(\mathcal{H}_A)$ klasszikus-kvantum állapot:

$$\varrho_{XA} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \varrho_x \tag{7.26}$$

és legyen $\sigma_{XA} = (\mathrm{id}_{\ell^1(\mathcal{X})}\otimes T)(\varrho_{XA})$, $\sigma_x = T(\varrho_x)$.

Rögzített $\varepsilon, \delta > 0$ és tetszőleges $n \in \mathbb{N}$ mellett legyen

$$A_\delta^{(n)} = \{(x_1 \dots x_n) \in \mathcal{X}^n | 2^{-n(H(P_X)+\delta)} \leq P(x_1)\dots P(x_n) \leq 2^{-n(H(P_X)-\delta)}\} \tag{7.27}$$

és tekintsük azt a $Q : \mathcal{X}^n \to [0,1]$ eloszlást, amire

$$Q(x) = \begin{cases} \frac{P_X^n(x)}{\sum_{x'\in A_\delta^{(n)}} P_X^n(x')} & \text{ha } x \in A_\delta^{(n)} \\ 0 & \text{egyébként}\end{cases} \tag{7.28}$$

ekkor elég nagy n-re $Q \leq \frac{P_X^n}{1-\varepsilon}$ teljesül.

Legyen $\sigma_B = \sum_{i\in I} p_i |i\rangle\langle i|$,

$$B_\delta^{(n)} = \{(i_1 \dots i_n) \in I^n | 2^{-n(H(B)_\sigma+\delta)} \le p_{i_1} \dots p_{i_n} \le 2^{-n(H(B)_\sigma-\delta)}\} \tag{7.29}$$

és

$$\Pi = \sum_{(i_1\dots i_n)\in B_\delta^{(n)}} |i_1 \dots i_n\rangle\langle i_1 \dots i_n| \tag{7.30}$$

Végül legyen $x \in \mathcal{X}$ esetén $\sigma_x = \sum_{i\in I_x} p_{x,i}|x,i\rangle\langle x,i|$, $x = (x_1, \dots, x_n) \in \mathcal{X}^n$ esetén

$$B_{x,\delta}^{(n)} = \{(i_1 \dots i_n) \in I_{x_1} \times \dots \times I_{x_n} | 2^{-n(H(B|X)_\sigma+\delta)} \le p_{x_1,i_1} \dots p_{x_n,i_n} \le 2^{-n(H(B|X)_\sigma-\delta)}\} \tag{7.31}$$

és

$$\Pi_x = \sum_{(i_1\dots i_n)\in B_{x,\delta}^{(n)}} |x_1, i_1 \dots x_n, i_n\rangle\langle x_1, i_1 \dots x_n, i_n| \tag{7.32}$$

Ha n elég nagy, akkor $x = (x_1, \dots, x_n) \in \mathcal{X}^n$ esetén $\sigma_x = \sigma_{x_1} \otimes \dots \otimes \sigma_{x_n}$ jelöléssel a nagy számok gyenge törvénye szerint a következők teljesülnek:

$$\operatorname{Tr}(\sigma_x \Pi) \ge (1-\varepsilon) \tag{7.33}$$

$$\operatorname{Tr}(\sigma_x \Pi_x) \ge (1-\varepsilon) \tag{7.34}$$

$$\operatorname{Tr} \Pi_x \le 2^{n(H(B|X)_\sigma+\delta)} \tag{7.35}$$

$$\tag{7.36}$$

A pakolási lemmát szeretnénk használni a Q eloszlással és a $(\sigma_x)_{x\in\mathcal{X}^n}$ állapotokkal, Π, $(\Pi_x)_{x\in\mathcal{X}^n}$ projektorokkal. A fenti három egyenlőtlenség a lemma négy feltétele közül három, a negyedikhez azt használjuk fel, hogy a

$$\sigma' := \sum_{x\in\mathcal{X}^n} Q(x)\sigma_x \tag{7.37}$$

állapotra $\sigma' \le \frac{\sigma_B}{1-\varepsilon}$ teljesül, ha n elég nagy. Eszerint

$$\begin{aligned} \Pi\sigma'\Pi &\le (1-\varepsilon)^{-1}\Pi\sigma_B\Pi \\ &\le (1-\varepsilon)^{-1}2^{-n(H(B)_\sigma-\delta)}\Pi \end{aligned} \tag{7.38}$$

A pakolási lemmából szerint bármely $\mathcal{M}$ halmazhoz létezik olyan $c : \mathcal{M} \to \mathcal{X}^n$ függvény és $(\Lambda_m)_{m\in\mathcal{M}\sqcup\{e\}}$ POVM, amire minden $m \in \mathcal{M}$ esetén

$$\operatorname{Tr} \sigma_{c_m}\Lambda_m \ge 1 - 4(\varepsilon + 2\sqrt{\varepsilon}) - 16(1-\varepsilon)^{-1}|\mathcal{M}|2^{n(H(B|X)_\sigma+\delta)-n(H(B)_\sigma-\delta)} \tag{7.39}$$

Legyen $\mathcal{M} = \{0,1\}^{\lfloor n(I(X;B)_\sigma-3\delta)\rfloor}$, c egy ilyen függvény, (Λ_m) ilyen POVM, és tekintsük az alábbi $E : \ell^1(\mathcal{M}) \to \mathcal{T}(\mathcal{H}_A^{\otimes n})$ és $D : \mathcal{T}(\mathcal{H}_B^{\otimes n}) \to \ell^1(\mathcal{M})$ csatornákat:

$$E(|m\rangle\langle m|) = \varrho_{c_m} \tag{7.40}$$

$$D(\varrho) = \sum_{m\in\mathcal{M}} (\operatorname{Tr}\Lambda_m\varrho)|m\rangle\langle m| + (\operatorname{Tr}\Lambda_e\varrho)\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}} |m\rangle\langle m| \tag{7.41}$$

Ekkor

$$\begin{aligned}\operatorname{Tr}\sigma_{c_m}\Lambda_m &\geq 1-4(\varepsilon+2\sqrt{\varepsilon})-16(1-\varepsilon)^{-1}2^{\lfloor n(I(X;B)_\sigma-3\delta)\rfloor}2^{n(H(B|X)_\sigma+\delta)-n(H(B)_\sigma-\delta)}\\ &\geq 1-4(\varepsilon+2\sqrt{\varepsilon})-16(1-\varepsilon)^{-1}2^{n(I(X;B)_\sigma+H(B|X)_\sigma-H(B)_\sigma-\delta)}\\ &= 1-4(\varepsilon+2\sqrt{\varepsilon})-16(1-\varepsilon)^{-1}2^{-n\delta}\\ &\geq 1-13\sqrt{\varepsilon}\end{aligned}\tag{7.42}$$

ha n elég nagy. Ezt felhasználva $m\in\{0,1\}^{\lfloor n(I(X;B)_\sigma-3\delta)\rfloor}$

$$\begin{aligned}&\left\|(D\circ T^{\otimes n}\circ E-cc^{\otimes\lfloor n(I(X;B)_\sigma-3\delta)\rfloor})(|m\rangle\langle m|)\right\|_1\\ &=\left\|\sum_{m'\in\mathcal{M}}(\operatorname{Tr}\Lambda_{m'}\sigma_{c_m})|m'\rangle\langle m'|+(\operatorname{Tr}\Lambda_e\sigma_{c_m})\frac{1}{|\mathcal{M}|}\sum_{m'\in\mathcal{M}}|m'\rangle\langle m'|-|m\rangle\langle m|\right\|_1\\ &\leq(1-\operatorname{Tr}\Lambda_m\sigma_{c_m})+\operatorname{Tr}\Lambda_e\sigma_{c_m}+\sum_{m'\neq m}\operatorname{Tr}\Lambda_{m'}\sigma_{c_m}\\ &\leq 2(1-\operatorname{Tr}\Lambda_m\sigma_{c_m})\leq 26\sqrt{\varepsilon}\end{aligned}\tag{7.43}$$

amiből a norma konvexitása miatt

$$\left\|D\circ T^{\otimes n}\circ E-cc^{\otimes\lfloor n(I(X;B)_\sigma-3\delta)\rfloor}\right\|_{1-1}\leq 26\sqrt{\varepsilon}\tag{7.44}$$

adódik. A klasszikus kapacitás definíciója szerint

$$\begin{aligned}C(T)=&\lim_{\varepsilon\to 0}\liminf_{n\to\infty}\frac{1}{n}\max\{m\in\mathbb{N}|\exists E:\ell^1(\{0,1\})^{\otimes m}\to\mathcal{T}(\mathcal{H}_A^{\otimes n}),\\ &\quad D:\mathcal{T}(\mathcal{H}_B^{\otimes n})\to\ell^1(\{0,1\})^{\otimes m}:\left\|D\circ T^{\otimes n}\circ E-cc^{\otimes m}\right\|_{1-1}<\varepsilon\}\\ \geq&\lim_{\varepsilon\to 0}\frac{1}{n}(\lfloor n(I(X;B)_\sigma-3\delta)\rfloor)\\ =&I(X;B)_\sigma-3\delta\end{aligned}\tag{7.45}$$

Ez minden $\delta>0$-ra és $\sigma=(\mathrm{id}_{\ell^1(\mathcal{X})}\otimes T)(\varrho_{XA})$ állapotra teljesül, tehát $C(T)\geq\chi(T)$. □

7.11. Következmény. *Ha $T:\mathcal{T}(\mathcal{H}_A)\to\mathcal{T}(\mathcal{H}_B)$ csatorna, akkor $C(T)\geq\chi_{reg}(T)$.*

Bizonyítás.

$$C(T)=\frac{1}{n}C(T^{\otimes n})\geq\frac{1}{n}\chi(T)\to\chi_{reg}(T)\tag{7.46}$$

□

7.12. Példa. Legyen $T = \mathrm{id}_{\mathcal{T}(\mathbb{C}^d)}$ az ideális qudit csatorna, ennek klasszikus kapacitása

$$C(T) = \chi(T) = \sup_{\varrho_{XA}} I(X;A)_\varrho = \log d \tag{7.47}$$

7.13. Tétel. *Legyenek $T_i : \mathcal{T}(\mathcal{H}_{A,i}) \to \mathcal{T}(\mathcal{H}_{B,i})$ csatornák ($i = 1,2$), és tegyük fel, hogy T_1 entanglement-breaking. Ekkor $\chi(T_1 \otimes T_2) = \chi(T_1) + \chi(T_2)$.*

Bizonyítás. Láttuk, hogy a Holevo-információ szuperadditív. A másik irányú egyenlőtlenséghez legyen $\varrho_{XA_1A_2} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \varrho_x$ olyan, hogy $\chi(T_1 \otimes T_2) = I(X;B_1B_2)_{(\mathrm{id}_{\ell^1(\mathcal{X})}\otimes(T_1\otimes T_2))(\varrho)}$. Ekkor $(T_1 \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{A,2})})(\varrho_x)$ szeparált, azaz felírható $\sum_{y\in\mathcal{Y}} P_{Y|X}(y|x)\sigma_{x,y} \otimes \tau_{x,y}$ alakban, ahol feltehető, hogy $\mathcal{Y}$ egy (x-től független) közös indexhalmaz. Legyen

$$\omega_{XYB_1B_2} = \sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} P_X(x)P_{Y|X}(y|x)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \sigma_{x,y} \otimes T_2(\tau_{x,y}) \tag{7.48}$$

Ekkor $\mathrm{Tr}_Y\,\omega = (\mathrm{id}_{\ell^1(\mathcal{X})} \otimes (T_1 \otimes T_2))(\varrho)$, és így

$$\begin{aligned}
\chi(T_1 \otimes T_2) &= I(X;B_1B_2)_\omega \\
&\leq I(XY;B_1B_2)_\omega \\
&= H(B_1B_2)_\omega - H(B_1B_2|XY)_\omega \\
&= H(B_1B_2)_\omega - H(B_1|XY)_\omega - H(B_2|XY)_\omega \\
&\leq H(B_1)_\omega + H(B_2)_\omega - H(B_1|XY)_\omega - H(B_2|XY)_\omega \\
&= I(XY;B_1)_\omega + I(XY;B_2)_\omega \\
&\leq \chi(T_1) + \chi(T_2)
\end{aligned} \tag{7.49}$$

felhasználva, hogy XY ismeretében ω feltételes állapota szeparált. □

7.14. Következmény. *Ha $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ entanglement-breaking csatorna, akkor $C(T) = \chi_{reg}(T) = \chi(T)$.*

7.15. Példa. Az $(S_{xy})_{x\in\mathcal{X},y\in\mathcal{Y}}$ sztochasztikus mátrixnak megfelelő $T_S : \ell^1(\mathcal{X}) \to \ell^1(\mathcal{Y})$

$$T_S(\varrho) = \sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} S_{xy}\langle x|\varrho|x\rangle|y\rangle\langle y| \tag{7.50}$$

csatorna entanglement-breaking.

Speciálisan az ideális klasszikus dit csatorna klasszikus kapacitása $\log d$.

17. HF. Legyen $\mathcal{X} = \mathcal{Y} = \{0,1\}$, $S_{xy} = (1-p)\delta_{xy} + p(1-\delta_{xy})$ a szimmetrikus bináris csatorna. Mi ennek a klasszikus kapacitása?

8. Összefonódással támogatott klasszikus kapacitás

- sűrű kódolás: ideális qubit csatorna kl kapacitása 1, de ha összefonódás is rendelkezésre áll, akkor 2

8.1. Példa. Legyen $\Phi = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) \in \mathcal{S}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, tegyük fel, hogy az egyik fele A-nál, a másik B-nél van. A alkalmazza a nála levő qubitre az $U \in \{I, \sigma_x, \sigma_y, \sigma_z\}$ unitér operátorok valamelyikét, azaz a $T_U : \varrho \mapsto U\varrho U^*$ csatornát. Ezután egy ideális qubit csatorna segítségével továbbítja B-nek, akinél így a $(T_U \otimes \mathrm{id}_{\mathcal{T}(\mathbb{C}^2)})(\Phi)$ állapot van. Ezek különböző U esetén egymásra ortogonálisak, tehát tökéletesen meg tudja különböztetni őket egy méréssel egymástól.

8.2. Definíció. Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna, $\varepsilon \in (0,1)$, és $m \in \mathbb{N}$. Legyen $\mathcal{H}_{E_A} \simeq \mathcal{H}_{E_B}$ Hilbert-tér. Egy $(\mathcal{E}, E, D)$ hármas a T-hez tartozó m bit ε-entangelement assisted-csatornakódolás, ha $\mathcal{E} : \mathbb{C} \to \mathcal{T}(\mathcal{H}_{E_A} \otimes \mathcal{K}_{E_B})$, $E : \ell^1(\{0,1\}^m) \otimes \mathcal{T}(\mathcal{H}_{E_A}) \to \mathcal{T}(\mathcal{H}_A)$, $D : \mathcal{T}(\mathcal{H}_B \otimes \mathcal{H}_{E_B}) \to \ell^1(\{0,1\}^m)$ csatornák és

$$\left\| D \circ (T \otimes \mathrm{id}_{\mathcal{H}_{E_B}}) \circ (E \otimes \mathrm{id}_{\mathcal{H}_{E_B}}) \circ (\mathrm{id}_{\ell^1(\{0,1\}^m)} \otimes \mathcal{E}) - cc^{\otimes m} \right\|_{1-1} \leq \varepsilon \quad (8.1)$$

8.3. Definíció. A $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna entanglement-assisted klasszikus kapacitása

$$C_{\mathrm{ent}}(T) = \lim_{\varepsilon \to 0} \liminf_{n \to \infty} \frac{1}{n} \sup \left\{ m \in \mathbb{N} | \exists T^{\otimes n}\text{-hez } m \text{ bit } \varepsilon\text{-e.a.-csatornakódolás} \right\} \quad (8.2)$$

8.4. Definíció. Egy $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna kölcsönös információja

$$I(T) = \sup_{\varrho_{A'A}} I(A;B)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'})} \otimes T)(\varrho)} \quad (8.3)$$

ahol a szuprémum tetszőleges $\varrho_{A'A} \in \mathcal{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_A)$ állapotokon értendő.

8.5. Tétel. *Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna és tegyük fel, hogy $0 < \varepsilon < \frac{1}{8}$ és (E, D) egy T-hez tartozó m bit ε-e.a.-csatornakódolás. Ekkor*

$$m \leq \frac{I(T) + 2h(\varepsilon)}{1 - 8\varepsilon} \quad (8.4)$$

Bizonyítás. Legyen $\Phi_{M_R M_A} = 2^{-m} \sum_{x \in \{0,1\}^m} |x\rangle\langle x| \otimes |x\rangle\langle x| \in \ell^1(\{0,1\}^m) \otimes \ell^1(\{0,1\}^m) = \Phi'_{M_R M_B}$, $\mathcal{E} : \mathcal{T}(\mathbb{C}) \to \mathcal{T}(\mathcal{H}_{E_A E_B})$, $E : \mathcal{T}(\mathcal{H}_{M_A E_A}) \to \mathcal{T}(\mathcal{H}_A)$,

$D : \mathcal{T}(\mathcal{H}_{E_B B}) \to \mathcal{T}(\mathcal{H}_{M_B})$, és tekintsük a következő állapotokat:

$$\varrho_{M_R A E_B} = (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{M_R})} \otimes E \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{E_B})}) \circ (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{M_R})} \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{M_A})} \otimes \mathcal{E})(\Phi_{M_R M_A}) \tag{8.5}$$

$$\sigma_{M_R B E_B} = (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{M_R})} \otimes T \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{E_B})})(\varrho) \tag{8.6}$$

$$\tau_{M_R M_B} = (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{M_R})} \otimes D)(\sigma) \tag{8.7}$$

Mivel (E, D) egy ε-e.a.-csatornakódolás, ezért $\|\Phi_{M_R M_B} - \tau_{M_R M_B}\|_1 \leq \varepsilon$. Emiatt

$$\begin{aligned}
m - 8\varepsilon m - 2h(\varepsilon) &\leq I(M_B; M_R)_\tau \\
&\leq I(BE_B; M_R)_\sigma \\
&= H(BE_B)_\sigma + H(M_R)_\sigma - H(BE_B M_R)_\sigma \\
&\quad + H(M_R E_B)_\sigma - H(M_R E_B)_\sigma + H(E_B)_\sigma \\
&\quad - H(E_B)_\sigma + H(B)_\sigma - H(B)_\sigma \\
&= I(M_R E_B; B)_\sigma + \underbrace{I(M_R; E_B)_\sigma}_{0} - I(B; E_B)_\sigma \\
&\leq I(M_R E_B; B)_\sigma \leq I(T)
\end{aligned} \tag{8.8}$$

□

8.6. Állítás. *A csatorna kölcsönös információja additív, azaz ha $T_i : \mathcal{T}(\mathcal{H}_{A_i}) \to \mathcal{T}(\mathcal{H}_{B_i})$ csatornák $(i = 1, 2)$, akkor $I(T_1 \otimes T_2) = I(T_1) + I(T_2)$.*

Bizonyítás. Legyen $\varrho_i \in \mathcal{S}(\mathcal{H}_{A'_i} \otimes \mathcal{H}_{A_i})$ olyan állapot, amire $I(A'_i; B_i)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'_i})} \otimes T_i)(\varrho_i)} = I(T_i)$. Ekkor

$$\begin{aligned}
I(T_1 \otimes T_2) &= \sup_{\varrho_{A' A_1 A_2}} I(A'; B_1 B_2)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'})} \otimes (T_1 \otimes T_2))(\varrho)} \\
&\geq I(A'_1 A'_2; B_1 B_2)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'_1})} \otimes T_1)(\varrho_1) \otimes (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'_2})} \otimes T_2)(\varrho_2)} \\
&= I(A'_1; B_1)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'_1})} \otimes T_1)(\varrho_1)} + I(A'_2; B_2)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'_2})} \otimes T_2)(\varrho_2)} \\
&= I(T_1) + I(T_2)
\end{aligned} \tag{8.9}$$

A másik irány bizonyításához legyen $\varrho \in \mathcal{S}(\mathcal{H}_{A' A_1 A_2})$ olyan tiszta állapot, amire $I(T_1 \otimes T_2) = I(A'; B_1 B_2)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'})} \otimes (T_1 \otimes T_2))(\varrho)}$ (konvexitás miatt létezik). Legyen $\tilde{T}_i : \mathcal{T}(\mathcal{H}_{A_i}) \to \mathcal{T}(\mathcal{H}_{B_i E_i})$ a T_i izometrikus kiterjesztése és

$$\phi = (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'})} \otimes (\tilde{T}_1 \otimes \tilde{T}_2))(\varrho) \in \mathcal{S}(\mathcal{H}_{A' B_1 E_1 B_2 E_2}) \tag{8.10}$$

$$\sigma = (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'})} \otimes (\tilde{T}_1 \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{A_2})}))(\varrho) \in \mathcal{S}(\mathcal{H}_{A' B_1 E_1 A_2}) \tag{8.11}$$

$$\tau = (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'})} \otimes (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A_1})} \otimes \tilde{T}_2))(\varrho) \in \mathcal{S}(\mathcal{H}_{A' A_1 B_2 E_2}) \tag{8.12}$$

Ekkor ϕ, σ, τ tiszta, tehát

$$
\begin{aligned}
I(T_1 \otimes T_2) =& I(A'; B_1B_2)_\phi \\
=& H(A')_\phi + H(B_1B_2)_\phi - H(AB_1B_2)\phi \\
=& H(B_1B_2E_1E_2)_\phi + H(B_1B_2)_\phi - H(E_1E_2) \\
=& H(B_1B_2|E_1E_2)_\phi + H(B_1B_2)_\phi \\
\leq& H(B_1|E_1)_\phi + H(B_2|E_2)_\phi + H(B_1)_\phi + H(B_2)_\phi \\
=& H(B_1E_1)_\phi + H(B_1)_\phi - H(E_1)_\phi \\
&+ H(B_2E_2)_\phi + H(B_2)_\phi - H(E_2)_\phi \\
=& H(A'A_2)_\sigma + H(B_1)_\sigma - H(A'A_2B_1)_\sigma \\
&+ H(A'A_1)_\tau + H(B_2)_\tau - H(A'A_1B_2)_\tau \\
=& I(A'A_2; B_1)_\sigma + I(A'A_1; B_2)_\tau \\
\leq& I(T_1) + I(T_2)
\end{aligned}
\tag{8.13}
$$

ahol $H(B_1B_2|E_1E_2) \leq H(B_1|E_1)+H(B_2|E_2)$ az erős szubadditivitás következménye. □

8.7. Következmény. *Tetszőleges $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna esetén $I(T^{\otimes k}) = kI(T)$, és így*

$$\lim_{k\to\infty} \frac{1}{k} I(T^{\otimes k}) = I(T) \tag{8.14}$$

8.8. Következmény. *Tetszőleges $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna esetén $C_{ent}(T) \leq I(T)$.*

8.9. Tétel. *Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna. Ekkor $C_{ent}(T) \geq I(T)$.*

Bizonyítás. (vázlat) Legyen $\mathcal{H}_{E_A} \simeq \mathcal{H}_{E_B} \simeq \mathcal{H}_A$ és $|\phi\rangle \in \mathcal{H}_{E_A} \otimes \mathcal{H}_{E_B}$ tetszőleges egységvektor, $\Phi = |\phi\rangle\langle\phi|$. Alkalmas $(|i\rangle_A)_{i\in I}$, $(|i\rangle_B)_{i\in I}$ ortonormált bázisokkal és $(p_i)_{i\in I}$ valószínűségi eloszlással

$$|\phi\rangle = \sum_i \sqrt{p_i} |i\rangle_A \otimes |i\rangle_B \tag{8.15}$$

írható. Ekkor

$$|\phi\rangle^{\otimes n} = \sum_{P\in\mathcal{P}_n(I)} \sqrt{p_{i_1}\cdots p_{i_n}} \sum_{(i_1,\ldots,i_n)\in T_P^n} |i_1\ldots i_n\rangle_A \otimes |i_1\ldots i_n\rangle_B \tag{8.16}$$

Itt $\mathcal{P}_n(I)$ az I^n-beli sorozatok típusainak halmaza, ahol egy $x : [n] \to I$ sorozat típusa az egyenletes eloszlás x szerinti előretoltja (tehát egy eloszlás I-n), T_P^n pedig a P típusú I^n-beli sorozatok halmaza.

Tekintsük minden d-re az $X : \mathbb{C}^d \to \mathbb{C}^d$, $|j\rangle \mapsto |j+1\rangle$ és $Z : \mathbb{C}^d \to \mathbb{C}^d$, $|j\rangle \mapsto e^{2\pi \frac{j}{d} i}$ unitér operátorokat. Ezekre $X^d = Z^d = I$ teljesül, tehát a kitevőt tekinthetjük $\mathbb{Z}_d$-beli elemnek is. Ha $x, z \in \prod_{P\in\mathcal{P}_n(I)} \mathbb{Z}_{|T_P^n|}$ és $b \in \{0,1\}^{\mathcal{P}_n(I)}$, akkor ezek segítségével megadhatunk egy

$$U(s) = \bigoplus_{P\in\mathcal{P}_n(I)} (-1)^{b_P} X^{x_P} Z^{z_P} \tag{8.17}$$

unitér operátort $\mathcal{H}_{E_A}$-n, ahol a tagok a típusosztályoknak megfelelő altereken hatnak (tetszőleges, de rögzített módon azonosítva $\mathbb{C}^{|T_P^n|}$-vel). Erre

$$(U(s)\otimes I)|\phi\rangle = (I\otimes U(s)^T)|\phi\rangle \tag{8.18}$$

teljesül, ahol a transzponálás az $(|i\rangle)_{i\in I}$ bázisokban értendő.

Legyen S az összes ilyen (x, z, b) hármas halmaza, és $s \in S$ esetén legyen

$$\begin{aligned}\sigma_s &= (T^{\otimes n}\otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{E_B})})((U(s)\otimes I)\Phi(U(s)\otimes I)^*)\\ &= (I\otimes U(s)^T)(T^{\otimes n}\otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{E_B})})(\Phi)(I\otimes U(s)^T)^*\end{aligned} \tag{8.19}$$

A pakolási lemmát szeretnénk használni a σ_s állapotokkal és az egyenletes eloszlással. Ekkor

$$\begin{aligned}\sigma &= \frac{1}{|S|}\sum_{s\in S}(I\otimes U(s)^T)(T^{\otimes n}\otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{E_B})})(\Phi)(I\otimes U(s)^T)^*\\ &= \sum_{P\in\mathcal{P}_n(I)}\ \sum_{(i_1,\dots,i_n)\in T_P^n} p_{i_1}\cdots p_{i_n} T^{\otimes n}(\pi_P)\otimes\pi_P\end{aligned} \tag{8.20}$$

ahol

$$\pi_P = \frac{1}{|T_P^n|}\sum_{i\in T_P^n}|i\rangle\langle i| \tag{8.21}$$

Legyen $\delta > 0$, $\Pi_{BE_B,n,\delta}$, $\Pi_{B,n,\delta}$ és $\Pi_{E_B,n,\delta}$ a $\varrho_{BE_B} := (T\otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_{E_B})})(\Phi)$, ϱ_B és ϱ_{E_B} állapotok n példányának megfelelő tipikus alterek projektorai. Legyen

$$\Pi_s = (I\otimes U(s)^T)^*\Pi_{BE_B,n,\delta}(I\otimes U(s)^T) \tag{8.22}$$

$$\Pi = \Pi_{B,n,\delta}\otimes\Pi_{E_B,n,\delta} \tag{8.23}$$

ekkor

$$\operatorname{Tr}\Pi\sigma_s \geq 1 \tag{8.24}$$

$$\operatorname{Tr}\Pi_s\sigma_s \geq 1 \tag{8.25}$$

$$\operatorname{Tr}\Pi_s \leq 2^{n(H(BE_B)_\varrho+\delta)} \tag{8.26}$$

$$\Pi\sigma\Pi \leq 2^{-n(H(B)_\varrho+H(E_B)_\varrho+\delta+o(1))}\Pi \tag{8.27}$$

$$\tag{8.28}$$

Emiatt elég nagy n-re a pakolási lemmából adódik, hogy lehet $n(H(B)_\varrho + H(E_B)_\varrho - H(BE_B)_\varrho - 3\delta) = n(I(B;E_B)_\varrho)$ bitet továbbítani $T^{\otimes n}$ és elegendően sok összefont állapot segítségével.

A maximális elérhető $I(B;E_B)_\varrho$ éppen a csatorna kölcsönös információja. □

8.10. Példa. Klasszikus csatorna kölcsönös információja megegyezik a Holevo-információval, tehát ilyenkor nem segít az összefonódás.

Ideális qudit csatorna kölcsönös információja $2 \log d$, tehát a sűrű kódolás optimális.

A $D_p(\varrho) = (1-p)(\varrho \oplus 0) + p(0 \oplus |e\rangle\langle e|)$ részleges törlő csatorna klasszikus kapacitása $2(1-p)\log d$

18. HF. Legyen $N_p : \mathcal{T}(\mathbb{C}^2) \to \mathcal{T}(\mathbb{C}^2)$ az a csatorna, amire $N_p(\varrho) = (1-p)\varrho + p\sigma_z\varrho\sigma_z$. Mutassuk meg, hogy $C_{\mathrm{ent}}(N_p) = 2 - h(p)$.

9. Kvantum kapacitás

9.1. Definíció. Legyen $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatorna, $\varepsilon \in (0,1)$ és $m \in \mathbb{N}$. Egy (E, D) pár a T-hez tartozó m qubit ε-csatornakódolás, ha $E : \mathcal{T}((\mathbb{C}^2)^{\otimes m}) \to \mathcal{T}(\mathcal{H})$, $D : \mathcal{T}(\mathcal{K}) \to \mathcal{T}((\mathbb{C}^2)^{\otimes m})$ csatornák és

$$\left\| D \circ T \circ E - qc^{\otimes m} \right\|_{\diamondsuit} \leq \varepsilon \tag{9.1}$$

9.2. Definíció. A $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna kvantum kapacitása

$$C_q(T) = \lim_{\varepsilon \to 0} \liminf_{n \to \infty} \frac{1}{n} \sup \left\{ m \in \mathbb{N} \middle| \exists T^{\otimes n}\text{-hez } m \text{ qubit } \varepsilon\text{-csatornakódolás} \right\} \tag{9.2}$$

9.3. Definíció. Egy $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna koherens információja

$$Q(T) = \sup_{\varrho_{A'A}} -H(A'|B)_{(\mathrm{id}_{\mathcal{T}(\mathcal{H}_{A'})} \otimes T)(\varrho)} \tag{9.3}$$

9.4. Tétel. *Legyen $T : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_B)$ csatorna. Ekkor*

$$C_q(T) = Q_{reg}(T) := \lim_{n \to \infty} \frac{1}{n} Q(T^{\otimes n}) \tag{9.4}$$

- teleportálás: ideális klasszikus bit csatorna kvantum kapacitása 0, de ha összefonódás is rendelkezésre áll, akkor lehet kvantuminformációt továbbítani
- entanglement-assisted kvantum kapacitás

10. Összefont állapotok és transzformációik

- összefont állapot: erőforrás, segítségével több információt lehet továbbítani
- ezeket hogyan lehet egymásba alakítani?

10.1. Definíció. Legyen K véges indexhalmaz, $\mathcal{H} = \bigotimes_{k\in K} \mathcal{H}_k$. Egy $\varrho \in \mathcal{S}(\mathcal{H})$ állapot szeparált, ha előáll $\bigotimes_{k\in K} \sigma_k$ alakú állapotok konvex kombinációjaként ($\sigma_k \in \mathcal{S}(\mathcal{H}_k)$). A nem szeparált állapotokat összefontnak nevezzük.

Ha $\mathcal{K} = \bigotimes_{k\in K} \mathcal{K}_k$, akkor egy $T : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ csatornát lokális operációnak nevezünk, ha $T = \bigotimes_{k\in K} T_k$ alakú, ahol $T_k : \mathcal{T}(\mathcal{H}_k) \to \mathcal{T}(\mathcal{K}_k)$ csatorna.

Ha $i, j \in K$, akkor a

$$cc_{ij} : \mathcal{T}\left((\mathbb{C}^2)_i \otimes \bigotimes_{k\in K\setminus\{i\}} \mathbb{C}\right) \to \mathcal{T}\left((\mathbb{C}^2(_j \otimes \bigotimes_{k\in K\setminus\{j\}} \mathbb{C}\right) \tag{10.1}$$

csatornát, amire

$$cc_{ij}(\varrho_i) = \langle 0|\varrho_i|0\rangle|0\rangle\langle 0|_j + \langle 1|\varrho_i|1\rangle|1\rangle\langle 1|_j \tag{10.2}$$

teljesül, az i-ből j-be haladó klasszikus kommunikációnak nevezzük.

Az olyan csatornákat, amelyek lokális operációkból és klasszikus kommunikációból előállnak véges számú tenzorszorzat és kompozíció segítségével, LOCC-nak nevezzük. Ezek halmazát $\mathrm{LOCC}(\mathcal{H}, \mathcal{K})$ jelöli, az összes $(\mathcal{H}, \mathcal{K})$ párra ezek uniójából álló osztály LOCC.

Ha $\varrho \in \mathcal{S}(\mathcal{H})$, $\sigma \in \mathcal{S}(\mathcal{K})$ és létezik $\Lambda \in \mathrm{LOCC}(\mathcal{H}, \mathcal{K})$, amire $\Lambda(\varrho) = \sigma$, akkor azt írjuk, hogy $\varrho \xrightarrow{\mathrm{LOCC}} \sigma$

- ha $\varrho \xrightarrow{\mathrm{LOCC}} \sigma$, akkor ϱ-t „erősebben összefontnak” tekinthetjük mint σ-t, mert ha LOCC az ingyenes manipulációkat modellezi, akkor ϱ minden olyan feladatra alkalmas, amire σ
- ha $\varrho \xrightarrow{\mathrm{LOCC}} \sigma$ és $\sigma \xrightarrow{\mathrm{LOCC}} \varrho$, akkor a két állapotot ugyanolyan hasznos erőforrásnak tekinthetjük

19. HF. Egy $\varrho \in \mathcal{H}$ állapot pontosan akkor szeparált, ha $1 \xrightarrow{\mathrm{LOCC}} \varrho$, ahol $1 \in \mathcal{S}(\bigotimes_{k\in K} \mathbb{C}) \simeq \mathcal{S}(\mathbb{C})$.

- a fenti interpretáció szerint a triviális $\varrho \xrightarrow{\mathrm{LOCC}} 1$ relációt figyelembe véve azt mondhatjuk, hogy az összes szeparált állapot egyforma az összefonódás szempontjából
- másik megközelítés: az összefonódott állapotokat jó ötlet LOCC segítségével összehasonlítani

10.2. Definíció. Legyen $\varrho, \sigma \in \mathcal{H}$,

$$\varrho = \sum_{i\in I} P(i)|i\rangle\langle i| \qquad \sigma = \sum_{i'\in I'} Q(i)|i'\rangle\langle i'| \tag{10.3}$$

ahol $(|i\rangle)_{i\in I}$ és $(|i\rangle)_{i'\in I'}$ ortonormált bázisok.

Azt mondjuk, hogy σ majorálja ϱ-t ($\varrho \prec \sigma$), ha Q majorálja P-t.

10.3. Lemma. *Legyen $\varrho, \sigma \in \mathcal{H}$, ekkor $\varrho \preceq \sigma$ pontosan akkor teljesül, ha léteznek $(U_j)_{j\in J}$ unitér operátorok és $p : J \to [0,1]$ valószínűségi eloszlás, amivel*

$$\varrho = \sum_{j\in J} p_j U_j \sigma U_j^* \tag{10.4}$$

Feltehető, hogy ϱ és σ ugyanabban az $(|i\rangle)_{i\in I}$ bázisban diagonálisak, a diagonális elemek tehát éppen P illetve Q értékeiből állnak.

Ha $P \preceq Q$, akkor valamely $(\pi_j)_{j\in J}$ permutációkra és $p : J \to [0,1]$ eloszlásra

$$P = \sum_{j\in J} p_j \pi_j Q \tag{10.5}$$

tehát

$$\varrho_A = \sum_{j\in J} p_j \pi_j \sigma_A \pi_j^* \tag{10.6}$$

Ha viszont

$$\varrho_A = \sum_{j\in J} p_j U_j \sigma_A U_j^* \tag{10.7}$$

akkor

$$\begin{aligned}\langle i|\varrho_A|i\rangle &= \sum_{j\in J}\sum_{i',i''\in I} p_j \langle i|U_j|i'\rangle\langle i'|\sigma_A|i''\rangle\langle i''|U_j^*|i\rangle \\ &= \sum_{j\in J}\sum_{i'\in I} p_j \langle i|U_j|i'\rangle\langle i'|\sigma_A|i'\rangle\langle i'|U_j^*|i\rangle \\ &= \sum_{i'\in I}\sum_{j\in J} p_j |\langle i|U_j|i'\rangle|^2\langle i'|\sigma_A|i'\rangle\end{aligned} \tag{10.8}$$

Mivel $(|\langle i|U_j|i'\rangle|^2)_{i,i'\in I}$ bisztochasztikus, $P \preceq Q$.

10.4. Lemma. *Legyen $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, tegyük fel, hogy mindkettő tiszta és $\varrho \xrightarrow{\text{LOCC}} \sigma$. Ekkor létezik $m \in \mathbb{N}$, $T_M : \mathcal{T}(\mathcal{H}_A) \to \mathcal{T}(\mathcal{H}_A) \otimes \ell^1(\{0,1\})^{\otimes m}$ csatorna, ami*

$$T_M(\varrho) = \sum_{j\in\{0,1\}^m} M_j \varrho M_j^* \otimes |j\rangle\langle j| \tag{10.9}$$

alakú és egy $T_U : \mathcal{T}(\mathcal{H}_B) \otimes \ell^1(\{0,1\})^{\otimes m} \to \mathcal{T}(\mathcal{H}_B)$ csatorna, ami

$$T_U(\varrho \otimes |j\rangle\langle j|) = U_j \varrho U_j^* \tag{10.10}$$

alakú, ahol U_j unitér, és amelyekre

$$\sigma = (\mathrm{id}_{\mathcal{T}(\mathcal{H}_A)} \otimes T_U) \circ (\mathrm{id}_{\mathcal{T}(\mathcal{H}_{AB})} \otimes cc_{AB}^{\otimes m}) \circ (T_M \otimes \mathrm{id}_{\mathcal{T}(\mathcal{H}_B)})(\varrho) \tag{10.11}$$

teljesül.

Tehát a transzformáció úgy is megvalósítható, hogy A végez egy mérést, az eredményt továbbítja B-nek, B pedig egy ettől függő unitér transzformációt hajt végre.

Bizonyítás. Feltehető, hogy a LOCC lépések során minden pillanatban

$$\sum_{x,y} P_{XY}(x,y)|x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \otimes \tau_{xy} \tag{10.12}$$

alakú, ahol $\tau_{xy} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ tiszta, mert egy

$$\varrho \otimes |x\rangle\langle x| \mapsto \sum_{i\in I} K_{x,i}\varrho K_{x,i}^* \otimes |x\rangle\langle x| \tag{10.13}$$

alakú lokális transzformációt mindig kicserélhetünk

$$\varrho \otimes |x\rangle\langle x| \mapsto \sum_{i\in I} K_{x,i}\varrho K_{x,i}^* \otimes |x\rangle\langle x| \otimes |i\rangle\langle i| \tag{10.14}$$

alakúra, és ha ϱ rangja 1, akkor $K_{x,i}\varrho K_{x,i}^*$ rangja is 1.

Emiatt elég azt megmutatni, hogy ha B mérést végez egy tiszta állapoton és az eredményt elküldi A-nak, az helyettesíthető azzal, hogy A végez mérést, elküldi az eredményt A-nak és B az eredménytől függően egy unitért transzformációt végez. Legyen a kiinduló állapot $|\psi\rangle\langle\psi|$

$$|\psi\rangle = \sum_{i\in I} \sqrt{p_i}|i\rangle_A \otimes |i\rangle_B \tag{10.15}$$

Ha $M \in \mathcal{B}(\mathcal{H}_B)$ egy Kraus-operátor,

$$M = \sum_{i,i'} M_{ii'}|i\rangle\langle i'|_B \tag{10.16}$$

akkor legyen

$$M' = \sum_{i,i'} M_{ii'}|i\rangle\langle i'|_A \tag{10.17}$$

Ekkor $(I \otimes M)|\psi\rangle$ és $(M' \otimes I)|\psi\rangle$ egymástól a A és B cseréjében és ezt követő lokális unitér transzformációban különböznek, tehát megegyeznek a Schmidt-együtthatóik. De ekkor a csere helyett másik lokális unitér transzformáció is megfelel, azaz $(I\otimes M)|\psi\rangle = (U_A\otimes U_B)(M'\otimes I)|\psi\rangle$. A helyettesítő Kraus-operátor (az A oldalon) tehát U_AM', az ezen kimenetelnek megfelelő unitér transzformáció (a B oldalon) U_B. □

10.5. Tétel (Nielsen)**.** *Legyen $K = \{A, B\}$, $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ tiszta állapotok. Ekkor $\varrho \xrightarrow{\text{LOCC}} \sigma$ pontosan akkor, ha σ_A majorálja ϱ_A-t.*

Bizonyítás. Tegyük fel, hogy $\varrho \xrightarrow{\text{LOCC}} \sigma$. A lemma szerint ekkor léteznek olyan $(M_j)_{j\in J}$ Kraus-operátorok és $(U_j)_{j\in J}$ unitérek, amivel

$$\sum_{j\in J}(M_j \otimes U_j)\varrho(M_j \otimes U_j)^* = \sigma \tag{10.18}$$

Mivel σ tiszta, ez csak úgy fordulhat elő, hogy minden j-re $(M_j \otimes U_j)\varrho(M_j \otimes U_j)^* = p_j\sigma$, tehát $M_j \varrho_A M_j^* = p_j \sigma_A$. Ekkor létezik olyan V_j unitér, amire $M_j\sqrt{\varrho_A} = \sqrt{p_j}\sqrt{\sigma_A}V_j$. Eszerint

$$\sqrt{\varrho_A}M_j^* M_j \sqrt{\varrho_A} = p_j V_j^* \sigma_A V_j \tag{10.19}$$

amiből

$$\varrho_A = \sum_{j\in J} \sqrt{\varrho_A} M_j^* M_j \sqrt{\varrho_A} = \sum_{j\in J} p_j V_j^* \sigma_A V_j \tag{10.20}$$

és így $\varrho_A \preceq \sigma_A$.

Most tegyük fel, hogy $\varrho_A \preceq \sigma_A$. Ekkor $\varrho_A = \sum_{j\in J} p_j U_j \sigma_A U_j^*$. Legyen $M_j = \sqrt{p_j}\sqrt{\sigma_A}U_j^* \varrho_A^{-1/2}$, M_0 pedig $(\operatorname{supp}\varrho_A)^\perp$ projektora, ekkor

$$\begin{aligned}\sum_{j\in J\sqcup\{0\}} M_j^* M_j &= M_0 + \varrho_A^{-1/2} \sum_{j\in J} p_j U_j \sigma_A U_j^* \varrho_A^{-1/2} \\ &= M_0 + \varrho_A^{-1/2} \varrho_A \varrho_A^{-1/2} = I\end{aligned} \tag{10.21}$$

Ha A alkalmazza az M_j-knek megfelelő mérést, akkor a kapott állapot redukált állapota σ_A lesz, tehát B oldalán egy alkalmas unitér transzformáció után σ az eredmény. □

10.6. Következmény. *Ha $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ tiszta és $\varrho \xrightarrow{\text{LOCC}} \sigma$, akkor $H(\varrho_A) \geq H(\sigma_A)$.*

Bizonyítás. A ϱ Schmidt-együtthatóiból alkotott valószínűségi eloszlás éppen ϱ_A sajátértékeiből áll (multiplicitással), ha Q majorálja P-t, akkor $H(P) \geq H(Q)$. □

20. HF. Mutassuk meg, hogy ha $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_{AB})$ tiszta állapotok és létezik $n \in \mathbb{N}$, hogy $\varrho \xrightarrow{\text{LOCC}} \sigma$, akkor létezik olyan $\tau \in \mathcal{S}(\mathcal{K}_{AB})$ tiszta állapot egy alkalmas Hilbert-téren, amire $\varrho \otimes \tau \xrightarrow{\text{LOCC}} \sigma \otimes \tau$.

- hasonló karakterizáció nem ismert kevert állapotokra vagy több részrendszer állapotaira
- itt is van értelme Shannon-típusú aszimptotikus viselkedést nézni: sok példány közelítő átalakítása LOCC segítségével

10.7. Definíció. Legyen $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$, $\mathcal{H} = \bigotimes_{k\in K} \mathcal{H}_k$. A $\varrho \to \sigma$ aszimptotikus LOCC transzformációs ráta

$$R(\varrho,\sigma) = \lim_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \inf\left\{m \in \mathbb{N} \middle| \exists \Lambda \in \operatorname{LOCC}(\mathcal{H}^{\otimes m}, \mathcal{H}^{\otimes n}) : \left\|\Lambda(\varrho^{\otimes m}) - \sigma^{\otimes n}\right\|_1 < \varepsilon\right\} \tag{10.22}$$

10.8. Állítás. *A szereplő állapotok tetszőleges megválasztása esetén a következők igazak:*

1. ha $\varrho \xrightarrow{\text{LOCC}} \sigma$*, akkor* $R(\varrho, \sigma) \leq 1$
2. $R(\varrho_1, \varrho_3) \leq R(\varrho_1, \varrho_2) R(\varrho_2, \varrho_3)$
3. $R(\varrho, \sigma_1 \otimes \sigma_2) \leq R(\varrho, \sigma_1) + R(\varrho, \sigma_2)$
4. $R(\varrho_1 \otimes \varrho_2, \sigma) \leq \frac{1}{\frac{1}{R(\varrho_1,\sigma)} + \frac{1}{R(\varrho_2,\sigma)}}$
5. $R(\varrho^{\otimes a}, \sigma^{\otimes b}) = \frac{b}{a} R(\varrho, \sigma)$
6. $R(\varrho, \sigma) \leq R(T(\varrho), \sigma)$ *tetszőleges* $T \in \text{LOCC}$ *esetén*
7. $R(\varrho, S(\sigma)) \leq R(\varrho, \sigma)$ *tetszőleges* $S \in \text{LOCC}$ *esetén*
8. $R(\varrho, \varrho) \in \{0, 1\}$

Bizonyítás. Legyen $\varrho \in \mathcal{H}$, $\sigma \in \mathcal{K}$ esetén

$$R_0^\varepsilon(\varrho, \sigma) = \inf \{ m \in \mathbb{N} | \exists \Lambda \in \text{LOCC}(\mathcal{H}^{\otimes m}, \mathcal{K}) : \left\| \Lambda(\varrho^{\otimes m}) - \sigma \right\|_1 < \varepsilon \} \tag{10.23}$$

Ekkor

$$R(\varrho, \sigma) = \lim_{\varepsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} R_0^\varepsilon(\varrho, \sigma^{\otimes n}) \tag{10.24}$$

1 Ha $\varrho \xrightarrow{\text{LOCC}} \sigma$, akkor $\varrho^{\otimes n} \xrightarrow{\text{LOCC}} \sigma^{\otimes n}$, tehát $R_0^\varepsilon(\varrho, \sigma^{\otimes n}) \leq n$.

2

$$R_0^{\varepsilon_1+\varepsilon_2}(\varrho_1, \varrho_3^{\otimes n}) \leq R_0^{\varepsilon_1}(\varrho_1, \varrho_2^{\otimes R_0^{\varepsilon_2}(\varrho_2, \varrho_3^{\otimes n})}) \tag{10.25}$$

miatt

$$\frac{1}{n} R_0^{\varepsilon_1+\varepsilon_2}(\varrho_1, \varrho_3^{\otimes n}) \leq \frac{1}{R_0^{\varepsilon_2}(\varrho_2, \varrho_3^{\otimes n})} R_0^{\varepsilon_1}(\varrho_1, \varrho_2^{\otimes R_0^{\varepsilon_2}(\varrho_2, \varrho_3^{\otimes n})}) \cdot \frac{1}{n} R_0^{\varepsilon_2}(\varrho_2, \varrho_3^{\otimes n}) \tag{10.26}$$

3

$$R_0^{\varepsilon_1+\varepsilon_2}(\varrho, \sigma_1 \otimes \sigma_2) \leq R_0^{\varepsilon_1}(\varrho, \sigma_1) + R_0^{\varepsilon_2}(\varrho, \sigma_2) \tag{10.27}$$

4

$$R_0^{\varepsilon_1+\varepsilon_2}(\varrho_1 \otimes \varrho_2, \sigma^{\otimes n_1+n_2}) \leq \max\{R_0^{\varepsilon_1}(\varrho_1, \sigma^{\otimes n_1}), R_0^{\varepsilon_2}(\varrho_2, \sigma^{\otimes n_2})\} \tag{10.28}$$

Legyen $\alpha = \frac{R(\varrho_2,\sigma)}{R(\varrho_1,\sigma)+R(\varrho_2,\sigma)}$, $n_1 = \lfloor \alpha n \rfloor$ és $n_2 = n - n_1$, majd $n \to \infty$, $\varepsilon_1, \varepsilon_2 \to 0$.

5

$$R_0^\varepsilon(\varrho^{\otimes a}, (\sigma^{\otimes b})^{\otimes n}) = \left\lceil \frac{1}{a} R_0^\varepsilon(\varrho, \sigma^{\otimes bn}) \right\rceil \tag{10.29}$$

alapján

$$\frac{1}{n} R_0^\varepsilon(\varrho^{\otimes a}, (\sigma^{\otimes b})^{\otimes n}) = \frac{1}{n} \left\lceil \frac{bn}{a} \frac{1}{bn} R_0^\varepsilon(\varrho, \sigma^{\otimes bn}) \right\rceil \tag{10.30}$$

6 $R_0^\varepsilon(\varrho, \sigma) \leq R_0^\varepsilon(T(\varrho), \sigma)$
7 $R_0^\varepsilon(\varrho, S(\sigma)) \leq R_0^\varepsilon(\varrho, \sigma)$
8 Az előzőek alapján $0 \leq R(\varrho, \varrho) \leq R(\varrho, \varrho)^2 \leq 1$.

□

Megjegyzés. $R(\varrho,\varrho)=0$ pontosan akkor, ha ϱ szeparált.

10.9. Lemma. *Legyen* $(|i\rangle_A)_{i\in I}$ *és* $(|i\rangle_B)_{i\in I}$ *ortonormált bázis* $\mathcal{H}_A$*-ban és* $\mathcal{H}_B$*-ben,* $P,Q:I\to[0,1]$ *valószínűségi eloszlások,*

$$\varrho=\sum_{i,i'\in I}\sqrt{P(i)P(i')}|i\rangle\langle i'|\otimes|i\rangle\langle i'| \tag{10.31}$$

és

$$\sigma=\sum_{i,i'\in I}\sqrt{Q(i)Q(i')}|i\rangle\langle i'|\otimes|i\rangle\langle i'| \tag{10.32}$$

Ekkor

$$\|\varrho-\sigma\|_1\leq 2\sqrt{\|P-Q\|_1} \tag{10.33}$$

Bizonyítás. Mivel ϱ és σ tiszta állapotok,

$$\begin{aligned}\|\varrho-\sigma\|_1&=2\sqrt{1-F(\varrho,\sigma)^2}\\&=2\sqrt{1-F(P,Q)^2}\\&\leq 2\sqrt{1-\left(1-\frac{1}{2}\|P-Q\|_1\right)^2}\\&\leq 2\sqrt{\|P-Q\|_1}\end{aligned} \tag{10.34}$$

□

10.10. Állítás. *Legyen* $\varrho\in\mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B)$ *tiszta és*

$$\Phi=\frac{1}{2}\left(|00\rangle+|11\rangle\right)\left(\langle 00|+\langle 11|\right) \tag{10.35}$$

Ekkor $R(\varrho,\Phi)\leq\frac{1}{H(\varrho_A)}$

Bizonyítás. Legyen $\varepsilon\in(0,1)$, $n\in\mathbb{N}$. Ekkor a lemma miatt létezik olyan ϱ' állapot, amire $\|\varrho^{\otimes n}-\varrho'\|_1\leq\varepsilon$ és $H_\infty^{\varepsilon^2/4}(\varrho_A^{\otimes n})=H_\infty(\varrho'_A)$.

A Nielsen-tétel miatt

$$\varrho'\xrightarrow{\text{LOCC}}\Phi^{\otimes\lfloor H_\infty(\varrho'_A)\rfloor}=\Phi^{\otimes\lfloor H_\infty^{\varepsilon^2/4}(\varrho_A^{\otimes n})\rfloor} \tag{10.36}$$

és így

$$\frac{1}{\lfloor H_\infty^{\varepsilon^2/4}(\varrho_A^{\otimes n})\rfloor}R_0^\varepsilon(\varrho,\Phi^{\otimes\lfloor H_\infty^{\varepsilon^2/4}(\varrho_A^{\otimes n})\rfloor})\leq\frac{n}{\lfloor H_\infty^{\varepsilon^2/4}(\varrho_A^{\otimes n})\rfloor} \tag{10.37}$$

$\lim_{\varepsilon\to 0}\limsup_{n\to\infty}$ után kapjuk az állítást. □

10.11. Állítás. *Legyen* $\sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ *tiszta és*

$$\Phi = \frac{1}{2}\left(|00\rangle + |11\rangle\right)\left(\langle 00| + \langle 11|\right) \tag{10.38}$$

Ekkor $R(\Phi, \sigma) \le H(\sigma_A)$

Bizonyítás. Legyen $\varepsilon \in (0,1)$, $n \in \mathbb{N}$. Ekkor a lemma miatt létezik olyan σ' állapot, amire $\|\sigma^{\otimes n} - \sigma'\|_1 \le \varepsilon$ és $H_0^{\varepsilon^2/4}(\sigma_A^{\otimes n}) = H_\infty(\sigma'_A)$.

A Nielsen-tétel miatt

$$\Phi^{\otimes \lfloor H_0^{\varepsilon^2/4}(\sigma_A^{\otimes n})\rfloor} = \Phi^{\otimes \lfloor H_0(\sigma'_A)\rfloor} \xrightarrow{\text{LOCC}} \sigma' \tag{10.39}$$

és így

$$\frac{1}{n} R_0^{\varepsilon}(\Phi, \sigma^{\otimes n}) \le \frac{\lfloor H_0^{\varepsilon^2/4}(\sigma_A^{\otimes n})\rfloor}{n} \tag{10.40}$$

$\lim_{\varepsilon\to 0} \limsup_{n\to\infty}$ után kapjuk az állítást. □

10.12. Tétel. *Legyen* $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ *tiszta. Ekkor*

$$R(\varrho, \sigma) = \frac{H(\sigma_A)}{H(\varrho_A)} \tag{10.41}$$

Bizonyítás.

$$\begin{aligned} 1 = R(\varrho, \varrho) &\le R(\varrho, \sigma) R(\sigma, \varrho) \\ &\le R(\varrho, \Phi) R(\Phi, \sigma) R(\sigma, \Phi) R(\Phi, \varrho) \\ &\le \frac{1}{H(\varrho_A)} H(\sigma_A) \frac{1}{H(\sigma_A)} H(\varrho_A) = 1 \end{aligned} \tag{10.42}$$

tehát itt mindenhol egyenlőség van. □

10.13. Definíció. Legyen $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ tetszőleges, és

$$\sigma = \frac{1}{2}\left(|00\rangle + |11\rangle\right)\left(\langle 00| + \langle 11|\right) \tag{10.43}$$

Ekkor ϱ entanglement costja $E_c(\varrho) = R(\sigma, \varrho)$ és a ϱ distillable entanglementje $E_d(\varrho) = \frac{1}{R(\varrho,\sigma)}$.

Megjegyzés. Az előbbiek alapján tiszta $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ esetén $E_c(\varrho) = E_d(\varrho) = H(\varrho_A)$

10.14. Definíció. Legyen $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ tetszőleges. A ϱ entanglement of formation-je

$$\begin{aligned} E_f(\varrho) = \inf \{ &\sum_{i\in I} p_i H(\operatorname{Tr}_B |\psi_i\rangle\langle\psi_i|) \big| \forall i \in I : \\ &p_i \in [0,1], \psi_i \in \mathcal{H}_A \otimes \mathcal{H}_B, \|\psi_i\| = 1, \sum_{i\in I} p_i |\psi_i\rangle\langle\psi_i| = \varrho \} \end{aligned} \tag{10.44}$$

Megjegyzés. Ha ϱ_{AB} tiszta, akkor $E_f(\varrho) = H(\varrho_A) = H(\varrho_B)$.

10.15. Állítás. *Legyen* $\varrho, \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, *és tegyük fel, hogy* $\varrho \xrightarrow{\text{LOCC}} \sigma$. *Ekkor* $E_f(\varrho) \geq E_f(\sigma)$.

10.16. Állítás. *Legyen* $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ *és* $\varrho, \sigma \in \mathcal{S}(\mathcal{H})$. *Ekkor*

$$|E_f(\varrho) - E_f(\sigma)| \leq 5d(\varrho, \sigma) \log \dim \mathcal{H} + 2 \tag{10.45}$$

ahol $d(\varrho, \sigma) = 2\sqrt{1 - F(\varrho, \sigma)}$.

10.17. Tétel. *Legyen* $\varrho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$. *Ekkor*

$$E_c(\varrho) = \lim_{n \to \infty} \frac{E_f(\varrho^{\otimes n})}{n} \tag{10.46}$$