QUICK NOTES

§2 Kitaev's framework.

§2.1 1st Kitaev's FrWrk.

- $\mathcal{A}, \mathcal{M}, \mathcal{B}$
- n even
- $|\Psi_0\rangle = |\Psi_{A,0}\rangle \otimes |\Psi_{M,0}\rangle \otimes |\Psi_{B,0}\rangle$
- $U_1 \dots U_n$; $U_i = \begin{cases} U_{A_i} \otimes \mathbb{1}_B & \text{odd} \\ \mathbb{1}_A \otimes U_{B,i} & \text{even} \end{cases}$

- $\{\Pi_{A,0}, \Pi_{A,1}\}$ POVM on $\mathcal{A}$; recall 0 means Alice won

  $\{\Pi_{B,0}, \Pi_{B,1}\}$ -- $\mathcal{B}$

- $\Pi_{A,1} \otimes \mathbb{1} \otimes \Pi_{B,0} |\Psi_n\rangle = \Pi_{A,0} \otimes \mathbb{1} \otimes \Pi_{B,1} |\Psi_n\rangle = 0$ for $|\Psi_n\rangle = U_n \dots U_1 |\Psi_0\rangle$.

Protocol.

1. Alice with $\mathcal{A}$, Bob with $\mathcal{M} \otimes \mathcal{B}$. $|\Psi_0\rangle$ init.
2. For $i = 1$ to n

   Alice $U_{A,i}$ i odd

   Bob $U_{B,i}$ i even.
3. $\mathcal{A}$ with $\{\Pi_{A,0}, \Pi_{A,1}\}$ & $\mathcal{B}$ with $\{\Pi_{B,0}, \Pi_{B,1}\}$.

NB: When honest, $|\Psi_i\rangle = U_i \dots U_1 |\Psi_0\rangle$

Final

$$P_A = |\Pi_{A,0} \otimes \mathbb{1} \otimes \Pi_{B,0} |\Psi_n\rangle|^2 = \mathrm{tr}\left(\Pi_{B,0}\, \mathrm{tr}_{A\otimes M} |\Psi_n\rangle\langle\Psi_n|\right)$$

$$P_B = |\Pi_{A,1} \otimes \mathbb{1} \otimes \Pi_{B,1} |\Psi_n\rangle|^2 = \mathrm{tr}\left(\Pi_{A,1}\, \mathrm{tr}_{M\otimes B} |\Psi_n\rangle\langle\Psi_n|\right)$$

using ✦ & $\mathbb{1} = \Pi_{A,0} + \Pi_{A,1}$ for the second inequality.

& $P_A + P_B = 1$ also follows.

$$\mathrm{tr}\left((\Pi_{A,1} + \Pi_{A,0}) \otimes \mathbb{1} \otimes (\Pi_{B,0} + \Pi_{B,1}) |\Psi\rangle\langle\Psi|\right) = 1$$

$$\parallel$$

$$P_A + P_B$$

- Impose $P_A (\Rightarrow P_B) = \frac{1}{2}$ for a standard coinflip.

When message qubits are flying:

$\sigma_{A,i} = \mathrm{tr}_{M\otimes B} |\Psi_i\rangle\langle\Psi_i|$ $\sigma_{B,i} = \mathrm{tr}_{A\otimes M} |\Psi_i\rangle\langle\Psi_i|$

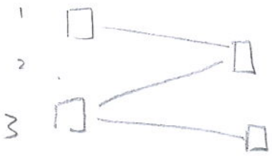
for honest players.

§ 2.1.1 Primal SDP.

Honest Alice; Cheating Bob.

$\rho_{A,0} = |\psi_{A,0}\rangle\langle\psi_{A,0}|$ (assume Alice prepares the 0^{th} message)

1) Bob can't affect Alice's qubits.



$\Rightarrow \quad \rho_{A,i} = \rho_{A,i-1}$ (i even)

NB: True even if Bob measures; Alice doesn't know the output (mixed state).

2) Alice performs a unitary.

[Let $\tilde{\rho}_{A,i}$ be the state on $A \otimes M$ after receiving the i^{th} message.

$\quad tr_M \tilde{\rho}_{A,i} = \rho_{A,i}$ (i even)

NB: Valid even if Bob sent the output of his measurement.

Alice applies the unitary and sends off M.

$$\rho_{A,i} = tr_M [U_{A,i} \tilde{\rho}_{A,i-1} U^{+}_{A,i}] \quad (i \text{ odd})$$

3) P_{win} (of Bob) $= tr(\Pi_{A,1} \rho_{A,n})$

$$P^*_B \leq \max_{\substack{\rho, \tilde{\rho} \\ s.t. (1) \& (2)}} tr(\Pi_{A,1} \rho_{A,n})$$

NB: Bound is tight: $|\phi_{i-1}\rangle \rightarrow \rho_{A,i-1}$

Bob wants $\rho_{A,i}$. For i even, trivial.
For i odd, the right $\tilde{\rho}_{A,i}$ must be sent.
Let $|\tilde{\phi}_i\rangle \rightarrow \tilde{\rho}_{A,i}$ but $tr(\tilde{\rho}_{A,i}) = \rho_{A,i}$ i odd
$\Rightarrow$ $|\tilde{\phi}_i\rangle$ & $|\phi_i\rangle$ are unitarily related.
Hence each cheating strategy is achievable.

§ 2.1.2 Dual SDP.

Hard to find optimal strategies. It's enough for us to find a bound. Dual SDP.

Certificates: upper bounds on P_B^*

↳ dual feasible points.

$$\mathrm{tr}(Z_{A,i-1}\,\rho_{A,i-1}) \geq \mathrm{tr}(Z_{A,i}\,\rho_{A,i}) \quad \text{(see rough)}$$

$$+ \qquad Z_{A,n} \geq \Pi_{A,1}$$

Let ρ^* be an optimal cheating strategy.

$$\Rightarrow \langle \psi_{A,0}|\, Z_{A,0}\, |\psi_{A,0}\rangle = \mathrm{tr}[Z_{A,0}\,\rho^*_{A,0}] \geq \mathrm{tr}[Z_{A,n}\,\rho^*_{A,n}] = P^*_B$$

↑ we know regardless of the cheating strategy.

$$Z_{A,i-1} \otimes \mathbb{1} \geq U^\dagger_{A,i}\,(Z_{A,i} \otimes \mathbb{1})\,U_{A,i}$$

$$Z_{A,i-1} = Z_{A,i}$$

↳ rough is neater, ironically.

Lemma 3: $Z_{A,0} \ldots Z_{A,n}$ for a protocol P constitutes a proof of upper bound $\langle \psi_{A,0}|\, Z_{A,0}\, |\psi_{A,0}\rangle \geq P^*_B$.

claim: (strong duality holds).

§ 2.2 Upper-Bounded Protocols.

Goal: Optimize over certificates & protocols.

Def^n: UBP

$$Z_{A,0}|\psi_{A,0}\rangle = \beta|\psi_{A,0}\rangle \qquad Z_{B,0}|\psi_{B,0}\rangle = \alpha|\psi_{B,0}\rangle$$

$$Z_{A,i-1} \otimes \mathbb{1}_M \geq U^\dagger_{A,i}(Z_{A,i} \otimes \mathbb{1}_M)U_{A,i} \qquad Z_{B,i-1} = Z_{B,i} \quad (i \text{ odd})$$

$$Z_{A,i-1} = Z_{A,i} \qquad \mathbb{1}_M \otimes Z_{B,i-1} \geq U^\dagger_{B,i}(\mathbb{1}_M \otimes Z_{B,i})U_{B,i} \quad (i \text{ even})$$

$$Z_{A,n} = \Pi_{A,1} \qquad Z_{B,n} = \Pi_{B,0}$$

Thm 5: $P^*_B \leq \beta$, $P^*_A \leq \alpha$.

NB: β & α are swapped. ∵ cheating for Alice is computed using Bob's quantities and ↔.

Why eigenvectors are OK?

claim: $\forall\ \epsilon > 0\ \exists\ \Lambda > 0$ s.t.

$$\left(\langle\psi_{A,0}|\, Z_{A,0}\, |\psi_{A,0}\rangle + \epsilon\right) |\psi_{A,0}\rangle\langle\psi_{A,0}| + \Lambda\left(I - |\psi_{A,0}\rangle\langle\psi_{A,0}|\right) \geq Z_{A,0}$$

NB: The LHS is an eigenvector of $|\psi_{A,0}\rangle$.

Thm 6: $f(\beta,\alpha) : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ s.t. $f(\alpha',\beta') \geq f(\alpha,\beta)$

whenever ~~f~~ $\alpha' \geq \alpha$ & $\beta' \geq \beta$ then

$$\inf_{\text{proto}} f(P^*_B, P^*_A) = \inf_{\text{UBP}} f(\beta,\alpha)$$

NB: In particular, optimal bias $f(\beta,\alpha) = \max(\beta,\alpha) - \frac{1}{2}$ can be found by optimizing either side. (DOUBT)

§ 2.2.1 Lower bounds & operator monotone functions

$$\langle\psi_{i-1}|\, Z_{A,i-1} \otimes \mathbb{1} \otimes Z_{B,i-1}\, |\psi_{i-1}\rangle \geq \quad (i \text{ odd})$$

$$\underbrace{\langle\psi_{i-1}|\left(U^\dagger_{A,i} \otimes \mathbb{1}_B\right)}\, Z_{A,i} \otimes \mathbb{1}_M \otimes Z_{B,i} \underbrace{\left(U_{A,i} \otimes \mathbb{1}_B\right)|\psi_{i-1}\rangle}$$

$$= \langle\psi_i|\, Z_{A,i} \otimes \mathbb{1}_M \otimes Z_{B,i}\, |\psi_i\rangle$$

Iterating

$$\beta\alpha = \langle\psi_0|\, Z_{A,0} \otimes \mathbb{1}_M \otimes Z_{B,0}\, |\psi_0\rangle \geq \langle\psi_n|\, Z_{A,n} \otimes \mathbb{1}_M \otimes Z_{B,n}\, |\psi_n\rangle$$

$$= \langle\psi_n|\, \Pi_{A,1} \otimes \mathbb{1}_M \otimes \Pi_{B,0}\, |\psi_n\rangle = 0$$

$\Rightarrow P^*_B P^*_A \geq 0$ (dissappointing but for strong coin flipping $P^*_B P^*_A \geq 1/2$ which is Kitaev's bound)

Can be made useful by using operator monotone f^n $f: [0,\infty) \to (0,\infty)$

which are s.t. $\forall$ $X \geq Y \Rightarrow f(X) \geq f(Y)$

(Their def^n from real # to matrices is extended by defining them on their diagonal forms, as usual) e.g. $f(z) = 1$

$f(z) = z$

counter: $f(z) = z^2$

e.g. $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \geq \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

but $\begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} \not\geq \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$

How are they helpful?

- $\langle \psi_i | Z_{A,i} \otimes \mathbb{1} \otimes f(Z_{B,i}) | \psi_i \rangle$ still the chain holds

$\Rightarrow \quad \beta f(\alpha) \geq P_B f(0)$; $\quad f(z) = 1 \Rightarrow$

$P^*_B \geq P_B$. (better than $P^*_A P^*_B \geq 0$, arguably).

- $\langle \psi_i | f(Z_{A,i}) \otimes \mathbb{1} \otimes g(Z_{B,i}) | \psi_i \rangle$?

Def^n. Bi-operator monotone f^n.

$f(x,y) : \mathbb{R}^+_0 \otimes \mathbb{R}^+_0 \longrightarrow \mathbb{R}^+_0$ acts as op. monotone in one var. when the other is fixed.

ie $\forall \; c \in \mathbb{R}^+$, $f(c, z) : \mathbb{R}^+_0 \to \mathbb{R}^+$ is op. mon.

& $f(z, c) : \mathbb{R}^+ \to \mathbb{R}^+$ . . . .

Further

- For $X = \sum_i x_i |x_i\rangle\langle x_i|$ $\quad Y = \sum y_i |y_i\rangle\langle y_i|$

$$f(X,Y) = \sum_{i,j} f(x_i, y_j) |x_i\rangle\langle x_i| \otimes |y_j\rangle\langle y_j|$$

Prop:

(a) If $Y' > Y$, $\quad f(X, Y') \geq f(X, Y)$

(b) $f(X, UYU^+) = (\mathbb{1} \otimes U) f(X,Y) (\mathbb{1} \otimes U^+)$

(c) $f(X, \mathbb{1} \otimes Y) = f(X \otimes \mathbb{1}, Y)$

$\Rightarrow$ (mini claim) $\quad \langle \psi_{i-1} | f(Z_{A,i-1}, \mathbb{1} \otimes Z_{B,i-1}) | \psi_{i-1} \rangle \geq$

$\langle \psi_i | f(Z_{A,i}, \mathbb{1}_M \otimes Z_{B,i}) | \psi_i \rangle$

Lemma 8. $f(P_B^*, P_A^*) \geq P_B f(1,0) + P_A f(0,1)$

proof: see rough 2.

§ 2.2.2 Some more facts about Op. Mon. F^ns.

- If $f(z)$ & $g(z)$ are op. mon. (assume >0 always)

  Then $a f(z) + b g(z)$ is also $\forall\ a \geq 0,\ b \geq 0$.

- If $f(z)$ is op. mon on a domain (a, b) then

  $f(z-c)$ is op. mon. on $(a+c, b+c)$.

- Claim: $f(z) = -\frac{1}{z}$ is op. monotone.

  proof: $Y \geq X > 0 \Rightarrow I \geq Y^{-1/2} X Y^{-1/2}$

  $\Rightarrow I \leq (Y^{-1/2} X Y^{-1/2})^{-1} = Y^{1/2} X^{-1} Y^{1/2}$

  $\Rightarrow Y^{-1} \leq X^{-1}$

  $\Rightarrow -Y^{-1} \geq -X^{-1}$

  $\Rightarrow f(z) = -\frac{1}{z}$ is op. monotone.

  Shift & restrict to get

  - $f(z) = \frac{-1}{\lambda+z}$ $\lambda \in [0, \infty)$ will also work.
  - also when input is restricted to $[0, \infty)$.
  - range $-ve$; fix by adding 1 as $1 - \frac{\lambda}{\lambda+z} = \frac{z}{\lambda+z}$.
    (& scaling)

- Claim: $f(z) = z, 1$ & $\frac{z}{\lambda+z}$ span the "extremal" rays of the convex cone of op. mon. f^ns.

  : $\exists$ unique $c_1 \geq 0, c_2 \geq 0$ & $dw \geq 0$ for each $f: (0,\infty) \to [0,\infty)$ op. mon.

  dw: measure on λ

$$f(z) = c_1 + c_2 z + \int_0^\infty \frac{\lambda z}{\lambda + z} \, dw(\lambda)$$

with $\int_0^\infty \frac{\lambda}{1+\lambda} \, dw(\lambda) < \infty$.

NB: they're infinitely differentiable.

§ 2.3 Time Dependent Point Games

Goal: Strip off extra information, viz. basis choice

Idea: Use distⁿ over eigenvalues

Defⁿ: For a state σ & $Z = \sum z \overbrace{|z\rangle\langle z|}^{\Pi_z}$

$$p(z) \leftrightarrow \mathrm{Prob}(Z, \sigma) = \mathrm{tr}(|z\rangle\langle z| \sigma)$$

& for $|\psi\rangle$

$$p(z) \leftrightarrow \mathrm{Prob}(Z, |\psi\rangle) = \mathrm{tr}(|z\rangle\langle z| \, |\psi\rangle\langle\psi|)$$

Motivⁿ: $\mathrm{tr}(\sigma f(Z)) = \sum_z p(z) f(z)$

Extⁿ: $p(z_A, z_B) = \mathrm{tr}(|z_A\rangle\langle z_A| \otimes \mathbb{1} \otimes |z_B\rangle\langle z_B| \; |\psi\rangle\langle\psi|)$

$\mathrm{Prob}(Z_A, Z_B, |\psi\rangle)$

Notⁿ: $\{[z_i]\}$ basis of f's s.t. non-zero only at z_i & zero else.

e.g. $p = c_1 [z_1] + c_2 [z_2]$

Extⁿ: $\{[x, y]\}$

e.g. (a) $\mathrm{Prob}(Z_{A,0}, Z_{B,0}, |\psi_0\rangle) \leftrightarrow 1 \cdot [\beta, \alpha]$

(b) $\mathrm{Prob}(Z_{A,n}, Z_{B,n}, |\psi_n\rangle) \leftrightarrow p_B [1,0] + p_A [0,1]$

$$\left\{ \begin{array}{l} \langle\psi_n| \underbrace{\Pi^A_0} \otimes \Pi^B_0 |\psi_n\rangle \\ \\ \langle\psi_n|(0 \cdot \Pi^A_0 + 1 \cdot \Pi^A_1) \otimes (1 \cdot \Pi^B_0 + 0 \cdot \Pi^B_1)|\psi_n\rangle \\ \\ p(x, y) = p_B [1,0] + p_A [0,1] \end{array} \right\}$$

Comment: UBP $\rightsquigarrow$ movie of moving points.

$\Downarrow$

Point Games.

Convention: The reverse time convention: at $t=0$, $p_B[1,0] + p_A[0,1]$

at $t=n$, $1, [\beta, \alpha]$

: In general at $t=i$, use $Z_{A,n-i}$, $Z_{B,n-i}$ & $|\psi_{n-i}\rangle$.

Motiv^n: Start at known $\frac{1}{2}[1,0] + \frac{1}{2}[0,1]$ (for $p_B = p_A = \frac{1}{2}$)

& then arbitrary steps (end condition is $[\beta, \alpha]$).

Use: We had (of the form) $\mathrm{tr}(\overset{Z_{n-i}}{Z^i}\, \overset{\sigma_{n-i}}{\sigma^i}) \le \mathrm{tr}(Z^{i+1}\sigma^{i+1})$

$\Rightarrow \mathrm{tr}(f(Z^i)\sigma^i) \le \mathrm{tr}(f(Z^{i+1})\sigma^{i+1})$

$\Leftrightarrow \sum_z p_i(z) f(z) \le \sum_z p_{i+1}(z) f(z)$ $\forall f$ op. mon.

claim (proven soon): also sufficient when extended to the other player.

Def^n: valid transition: $p_i \to p_{i+1}$ valid iff

- $\sum_z p_i(z) = \sum_z p_{i+1}(z)$
- $\sum_z p_i(z) f(z) \le \sum_z p_{i+1}(z) f(z)$

[strictly valid

- $\sum_z p_i(z) f(z) < \sum_z p_{i+1}(z) f(z)$]

Lemma 11. $p_i \to p_{i+1}$ is valid iff

$$\sum_z (p_{i+1}(z) - p_i(z)) = 0 \quad \&$$

$$\sum_z \frac{\lambda z}{\lambda + z}(p_{i+1}(z) - p_i(z)) \ge 0 \quad \forall \lambda \ge 0$$

proof: fs char. by $\underset{\text{prob cons.}}{1}$, z & $\frac{\lambda z}{\lambda + z}$ (z: $\lambda \to \infty$ lt.)

Story: Similarly UBPs "$\Rightarrow$" will prove soon.

$$\sum_{x,y} p_i(x,y)\, f(x,y) \le \sum_{x,y} p_{i+1}(x,y)\, f(x,y)$$

f are bi-op. mon.

Def^n 12. Let $p_i(x,y)$ & $p_{i+1}(x,y)$, $\mathbb{R}^+ \otimes \mathbb{R}^+ \to \mathbb{R}^+$.

$p_i(x,y) \to p_{i+1}(x,y)$ is a valid transition if either

1) $\forall\, c \in \mathbb{R}^+$, $p_i(z,c) \to p_{i+1}(z,c)$ is valid

OR

2) $\forall\, c \in \mathbb{R}^+$, $p_i(c,z) \to p_{i+1}(c,z)$ is valid

horizontal tran^n (Alice applies a unitary)

vertical tran^n. (Bob applies a unitary)

"Def^n": Transitively Valid := 2 f^{n}s are trans valid if $\exists$ a sequence s.t. each transition is valid

Def^n 13. "A time dependent point game (TDPG)" is a seq. of $p_0(x,y), \ldots p_n(x,y)$ s.t

$p_i(x,y) \to p_{i+1}(x,y)$ is valid $\forall i$

& $p_0 = p_B[1,0] + p_A[0,1]$ &

$p_n = 1\,[\beta,\alpha]$

$[\beta,\alpha]$ is the final point of the TDPG.

TASK 1:

UBP $\Rightarrow$ TDPG.

NB: Initial & final states ✓

given a UBP, $p_i = \mathrm{Prob}(Z_{A,n-i}, Z_{B,n-i}, |\psi_{n-i}\rangle)$
& $p_{i+1} = \mathrm{Prob}(Z_{A,n-i-1}, Z_{B,n-i-1}, |\psi_{n-i-1}\rangle)$

Recall: UBP $\Rightarrow$ $Z_{A,n-i-1} \otimes \mathbb{1}_M \geq U^{\dagger}_{A,n-i} \left(Z_{A,n-i} \otimes \mathbb{1} \right) U_{A,n-i}$

$$Z_{B,n-i-1} = Z_{B,n-i}$$

& $|\Psi_{n-i}\rangle = U_{A,n-i} \otimes \mathbb{1}_B |\Psi_{n-i-1}\rangle$

Now expand $|\Psi_{n-i-1}\rangle = \sum_y |\phi_y\rangle \otimes |y\rangle$

unnormalized on $A \otimes M$ — norm. eigenvectors of $Z_{B,n-i}$

NB: $|\phi_y\rangle$ may not be orthogonal (its not a schmidt decomposition)

Fix y & $p_{i+1}(x,y) = \mathrm{Prob}\left(Z_{A,n-i-1}, \rho_{n-i-1,y}\right)$

where $\rho_{n-i-1,y} := \mathrm{tr}_M [\, |\phi_y\rangle\langle\phi_y| \,]$.

For $p_i(x,y) = \mathrm{Prob}\left(Z_{A,n-i}, \rho_{n-i,y}\right)$

$\rho_{n-i,y} := \mathrm{tr}_M \left[U_{A,n-i} |\phi_y\rangle\langle\phi_y| U^{\dagger}_{A,n-i} \right]$.

Can use the same proof as before (for a single var. trans.) to show

$p_i(x,y) \to p_{i+1}(x,y)$ is valid $\forall y$.

Similarly for x in $i+1 \to i+2$ & in general then

$p_i(x,y) \to p_{i+1}(x,y)$ is also valid

TASK 2:

TDPG $\Rightarrow$ UBP in the sense

$\forall$ TDPG with final point $[\beta, \alpha]$

$\exists$ a UBP with bound $(\beta+\epsilon, \alpha+\epsilon)$ for arb $\epsilon > 0$.

$\Rightarrow$ Inf of both are same.

Rough

$$\max_{\rho} \mathrm{tr}\Big(\pi_{A,1}\, \rho_{A,n} - \sum_i \big(Z_i \otimes \mathbb{1}\, \tilde\rho_{A,i} - Z_i \otimes \mathbb{1}\, U_{A,i} \tilde\rho_{A,i-1} U^\dagger_{A,i} \big)$$

$$- \sum_i \big(Z_i \otimes \mathbb{1}$$

$\rho_1 = |\psi\rangle\langle\psi|$

$\rho_2 = \rho_1$ A $\rho_1 = \rho_2$

$\rho_3 = \rho_2$ A $\rho_3 = \rho_4$

A $\rho_5 = \rho_6$

$$\cancel{\mathrm{tr}_M(\tilde\rho_2)} = \mathrm{tr}_M(\tilde\rho_3)$$

$$\rho_2 = \rho_3$$

$$\rho_2 = \mathrm{tr}\big(U_3 \tilde\rho_3 U_3\big)$$

$$\mathrm{tr}_M(\tilde\rho_3) = \mathrm{tr}_M\big(U_1 \tilde\rho_1 U_1^\dagger\big)$$

$$\mathrm{tr}_M(\tilde\rho_5) = \mathrm{tr}_M\big(U_3 \tilde\rho_3 U_3\big)$$

$\vdots$

$$\mathrm{tr}\Big(\quad \sum Z_i \otimes \mathbb{1}\, \tilde\rho_i - Z_i \otimes \mathbb{1}\, U_{i-2}\, \tilde\rho_{i-2}\, \tilde U^\dagger_{i-2}$$

$$U^\dagger_{i-2} Z_{i-2} \otimes \mathbb{1}\, U_{i-2} \big) \tilde\rho_i$$

$$\mathrm{tr}\big(\pi (Z_i \ldots \otimes \mathbb{1}) \rho_i \sum \big(Z_i \otimes \mathbb{1}$$

$$Z_{A,n} \geq \pi_{A,1}$$

$$U_i^\dagger Z_{A,i-1} U_i \geq Z_{A,i}$$

$$Y' = U Y U^{+} = \sum y_i |y'_i\rangle\langle y'_i|$$

$$Y = \sum y_i |y_i\rangle\langle y_i| \qquad y'_i = y_i$$

$\therefore$ eigenvalues preserved by U.

$$f(Y') = \sum f(y_i) \, |y'_i\rangle\langle y'_i|$$

$$= f(y_i) \, U |y_i\rangle\langle y_i| U^{+}$$

$$= U f(Y) U^{+}.$$

$$\langle\Psi| \, f\left(|B\rangle\langle B|, \mathbb{1} \otimes |A\rangle\langle A|\right) |\Psi\rangle$$

$$\cancel{\langle\Psi| \left(\sum f(x,y) \, |x\rangle\langle x| \otimes |y\rangle\langle y|\right) |\Psi\rangle}$$

$$\cancel{f(0,1) \, P_A^{*} P_B^{*}}$$

$$\langle\Psi_0| Z_0^A \otimes \mathbb{1} \otimes Z_0^B |\Psi_0\rangle \geq \langle\Psi_n| Z_n^A \otimes \mathbb{1} \otimes Z_n^B |\Psi_n\rangle$$

$$\langle\Psi_n| \Pi^{A,1} \otimes \mathbb{1} \otimes \Pi^{B,0} |\Psi_n\rangle$$

$$f(\alpha \, \mathrm{tr}(|\Psi_0\rangle\langle\Psi_0|) \otimes \mathbb{1} \otimes \beta \, \mathrm{tr}(|\Psi_0\rangle\langle\Psi_0|)$$

$$f(\alpha, \beta) \, \langle\Psi_0| \, \mathrm{tr}(|\Psi_0\rangle\langle\Psi_0|) \otimes \mathbb{1} \otimes \mathrm{tr}(|\Psi_0\rangle\langle\Psi_0|) \, |\Psi_0\rangle$$

$$\geq \langle\Psi_n| \, f(\underbrace{\Pi^{A,1}, \mathbb{1} \otimes \Pi^{B,0}}) \, |\Psi_n\rangle$$

$$f\left(|1\rangle\langle 1|, |0\rangle\langle 0|\right)$$

$$f\left(0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|, 1 \cdot |0\rangle\langle 0| + 0 \cdot |1\rangle\langle 1|\right)$$

$$f(0,1) \, |0\rangle\langle 0| \otimes |0\rangle\langle 0|$$

$$+ f(1,0) \, |1\rangle\langle 1| \otimes |1\rangle\langle 1|$$

$$+ f(0,0) \cdots + f(1,1) \cdots$$

$$= f(0,1) \, p^A + f(1,0) \, p^B$$

$f(z) \cancel{A} = (\frac{1}{z})$

$\cancel{\text{Is}} \overset{?}{\Rightarrow} f(Z) = Z^{-1}$?

Yes $\because$ say $Z = z|z\rangle\langle z|$.

$f(Z) = z^{-1} |z\rangle\langle z|$

$f(Z).Z = \sum_{z'} z^{-1} z' |z\rangle\langle z|z'\rangle\langle z'|$

$= |z\rangle\langle z|$.

also works in a different basis.

$\sum_z z \; U|z\rangle\langle z|U^+$

$-\frac{1}{z}$ (∞, ∞)

$-\frac{1}{\lambda+z}$ $(-\infty-\lambda, \infty-\lambda)$

$\frac{-1}{\lambda+z}$ $(0, \infty-\lambda)$