1. **Constructing entanglement witness from the partial transpose** (10 Points: 1+2+2+2+2+1)
In the lecture, we saw that every separable bi-partite quantum state has a positive partial transpose, which means that the positivity is an entanglement criterion. First, we show that this criterion is valid.

a) Show that for an arbitrary separable bi-partite quantum state $\rho = \sum_i p_j(\rho_{Ai} \otimes \rho_{Bi})$, all eigenvalues of ρ^{T_A} are greater than or equal to 0, i.e., $\rho^{T_A} \geq 0$.

- $\rho = \sum_i p_i \left(\rho_{Ai} \otimes \rho_{Bi}\right)$
- $\rho^{T_A} = \sum_i p_i \, \rho_{Ai}^T \otimes \rho_{Bi}$
- $\rho_{Ai} \geq 0 \Rightarrow \rho_{Ai}^T \geq 0$

$\rho_{Ai} = UDU^\dagger \Rightarrow \rho_{Ai}^T = U^* \underset{\underset{D}{\shortparallel}}{D^*} U^t = U^* \underset{\underset{0}{\rotatebox{90}{$\leq$}}}{D} U^{*\dagger}$

$\Rightarrow \rho_{Ai}^T \otimes \rho_{Bi} \geq 0$

The eigenvalues of $\rho_{Ai}^T \otimes \rho_{Bi}$ are the products of eigenvalues of ρ_{Ai}^T and ρ_{Bi}.

$\Rightarrow \rho^{T_A} = \sum_i \underset{\underset{0}{\rotatebox{90}{$\leq$}}}{p_i} \underbrace{\left(\rho_{Ai}^T \otimes \rho_{Bi}\right)}_{\geq 0} \Rightarrow \square$

$\langle v|\rho^{T_A}|v\rangle \geq 0 \;\; \forall v.$

- ρ sep $\Rightarrow \rho^{T_A} \geq 0$
- $\rho^{T_A} \ngeq 0 \Rightarrow \rho$ entangled
- $\rho^{T_A} \geq 0 \overset{??}{\Rightarrow} \rho$ sep ? No, there are states with $\rho^{T_A} \geq 0$ but entangled.

In general, the opposite direction is not true. However, if we restrict a quantum state to a pure state, the opposite is also true as the following.

b) Show that a bi-partite pure state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is separable if it has a positive partial transpose.

Hint: Prove the contraposition: if $|\psi\rangle$ is entangled, $(|\psi\rangle\langle\psi|)^{T_A}$ has at least one negative eigenvalue. To this end, use Schmidt decomposition.

· If a state is pure:

$\exists \; \{|u_i\rangle\}, \{|v_i\rangle\}$ orth. basis : $|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\, |u_i\rangle \otimes |v_i\rangle$

PROOF:

$|\psi\rangle = \sum_{i,j} C_{i,j} |i\rangle \otimes |j\rangle = \sum_{i,j} (UDV^\dagger)_{i,j} |i\rangle \otimes |j\rangle = \sum_{\ell} D_{\ell\ell} \left(\sum_i U_{i,\ell} |i\rangle\right) \otimes \left(\sum_j V^\dagger_{\ell,j} |j\rangle\right)$

$C = UDV^\dagger$ with $D \geq 0$ (SVD); $\sum_i U_{i,\ell}|i\rangle = U|\ell\rangle$, $\sum_j V^\dagger_{\ell,j}|j\rangle = V^*|\ell\rangle$

$= \sum_\ell \sqrt{\lambda_\ell}\; U|\ell\rangle \otimes V^*|\ell\rangle$, with $D_{\ell\ell} = \sqrt{\lambda_\ell}$, $U|\ell\rangle = |u_\ell\rangle$, $V^*|\ell\rangle = |v_\ell\rangle$

· $\sum_i \lambda_i = 1$

$\sum_i \lambda_i = \sum_i D_{ii}^2 = tr(D^\dagger D) = tr(C^\dagger C) = \sum_j \langle j|C^\dagger C|j\rangle = \sum_{i,j} \langle j|C^\dagger|i\rangle\langle i|C|j\rangle$, with $\langle j|C^\dagger|i\rangle = \langle i|C|j\rangle^*$

$= \sum_{i,j} |C_{i,j}|^2 = \langle\psi|\psi\rangle = 1$

$|\psi\rangle\langle\psi| = \sum_{i,j} \sqrt{\lambda_i \lambda_j}\; |u_i\rangle\langle u_j| \otimes |v_i\rangle\langle v_j|$

$(|\psi\rangle\langle\psi|)^{T_A} = \sum_{i,j} \sqrt{\lambda_i \lambda_j}\; |u_j\rangle^* \langle u_i|^* \otimes |v_i\rangle\langle v_j|$

· $(|u_i\rangle\langle u_j|)^t = (|u_i\rangle\langle u_j|)^{\dagger *} = (|u_j\rangle\langle u_i|)^*$

· Or without BRAKET $(\vec{u}_i \vec{u}_j^{\,\dagger})^t = \vec{u}_j^{\,*} \vec{u}_i^{\,t} = \vec{u}_j^{\,*} \vec{u}_i^{\,*\dagger} = |u_j^*\rangle\langle u_i^*|$, where $\vec{u}_i \vec{u}_j^{\,\dagger} = (|u_i\rangle\langle u_j|)^t$

· EIGENSTATES OF $(|\psi\rangle\langle\psi|)^{T_A}$:

· $|u_i^*\rangle \otimes |v_i\rangle$, λ_i (EIGENVALUE) ,

· $\dfrac{|u_i^*\rangle\otimes|v_j\rangle + |u_j^*\rangle\otimes|v_i\rangle}{\sqrt{2}}$, $\sqrt{\lambda_i \lambda_j}$ $\quad \forall\, i \neq j$

• $\frac{|u_i\rangle^* \otimes |v_j\rangle - |u_j\rangle^* \otimes |v_i\rangle}{\sqrt{2}}$, $\underbrace{-\sqrt{\lambda_i \lambda_j}}_{<0}$ $\forall i \neq j$

$|\Psi\rangle\langle\Psi|$ entangled $\Rightarrow$ More than one schmidt coefficient is $\neq 0$

$\Rightarrow \exists$ Negative eigenvalue of $(|\Psi\rangle\langle\Psi|)^{T_A}$

($\exists$ Negative eigenvalue of $(|\Psi\rangle\langle\Psi|)^{T_A}$ $\Rightarrow$ More than one schmidt coefficient is $\neq 0$.

$\Rightarrow$ $|\Psi\rangle\langle\Psi|$ entangled)

Recall that an entanglement witness is an observable W with the following conditions: (i) $\mathrm{Tr}(W\sigma) \geq 0$ for all separable states σ and (ii) there exists an entangled state $\tilde{\rho}$ satisfying $\mathrm{Tr}(W\tilde{\rho}) < 0$.

c) Consider an entangled state ρ. Let $|\mu\rangle$ be an eigenvector of ρ^{T_A} whose eigenvalue is negative. Then show that $W = (|\mu\rangle\langle\mu|)^{T_A}$ is an entanglement witness and $|\mu\rangle$ is an entangled state.

• $\underset{\uparrow \text{ eigendecomp.}}{\rho} = \sum \lambda_i |\Psi_i\rangle\langle\Psi_i|$ $\Rightarrow$ $\rho^{T_A} = \sum_i \lambda_i (|\Psi_i\rangle\langle\Psi_i|)^{T_A}$

PURE STATE $\Rightarrow$ Before we saw that $(|\Psi_i\rangle\langle\Psi_i|)^{T_A}$ is diagonalizable.

• $\rho : \rho^{T_A} \ngeq 0 \Rightarrow \exists\, |\mu\rangle : \rho^{T_A}|\mu\rangle = \lambda|\mu\rangle$ with $\lambda < 0$

• $W := (|\mu\rangle\langle\mu|)^{T_A}$

• σ sep. $\Rightarrow \mathrm{Tr}[W\sigma] = \mathrm{Tr}[(|\mu\rangle\langle\mu|)^{T_A}\sigma] = \mathrm{Tr}[|\mu\rangle\langle\mu|\sigma^{T_A}]$

$= \langle\mu|\sigma^{T_A}|\mu\rangle \geq 0$

σ SEP $\Rightarrow$ PPT. $(\sigma^{T_A} \geq 0)$

• $\tilde{\rho} := \rho$ is entangled and $\mathrm{Tr}[W\tilde{\rho}] = \mathrm{Tr}[|\mu\rangle\langle\mu|\tilde{\rho}^{T_A}] = \langle\mu|\tilde{\rho}^{T_A}|\mu\rangle = \lambda\langle\mu|\mu\rangle = \lambda < 0$

• $\mathrm{Tr}[W\tilde{\rho}] < 0 \Rightarrow W = (|\mu\rangle\langle\mu|)^{T_A} \ngeq 0 \Rightarrow |\mu\rangle$ entangled.

$\left(\mathrm{Tr}[W\tilde{\rho}] = \sum_i \tilde{\lambda}_i \mathrm{Tr}[W|v_i\rangle\langle v_i|] = \sum_i \tilde{\lambda}_i \langle v_i|W|v_i\rangle < 0 \Rightarrow \exists i : \langle v_i|W|v_i\rangle < 0 \Rightarrow W \ngeq 0 \right)$

As an application of this witness, we consider the following setting. In our (fictitious) lab, we are trying to prepare a two-qubit state $|\psi\rangle \in \mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$. We use a simple model[1] for what is actually happening in the lab, namely that we prepare a state with some noise

$$\rho(p) := p\,|\psi\rangle\langle\psi| + (1-p)\frac{\mathbb{1}}{4}.$$

Our goal is to have an observable witness that decides whether $\rho(p)$ is entangled or not. To this end, we will use the fact that for two-qubits system there exist no entangled. positive partial transpose (PPT) states. Therefore, the partial transpose T^A will always detect entanglement of $\rho(p)$.

d) Assume $|\psi\rangle = a\,|01\rangle_{AB} + b\,|10\rangle_{AB}$. Calculate eigenvalues of $\rho(p)^{T_B}$, and determine the values of p depending on a, b such that $\rho(p)$ is entangled.

Hint: Use the fact that $\rho(p)$ is entangled if and only if $\rho(p)^{T_B} \ngeq 0$.

- $|\psi\rangle\langle\psi| = |a|^2\,|01\rangle\langle 01| + ab^*\,|01\rangle\langle 10| + |b|^2\,|10\rangle\langle 10| + a^*b\,|10\rangle\langle 01|$

- $\rho(p) = p\left(|a|^2\,|01\rangle\langle 01| + ab^*\,|01\rangle\langle 10| + |b|^2\,|10\rangle\langle 10| + a^*b\,|10\rangle\langle 01|\right) + (1-p)\dfrac{\mathbb{1}}{4}$

- $\rho(p)^{T_B} = p\left(|a|^2\,|01\rangle\langle 01| + ab^*\,|00\rangle\langle 11| + |b|^2\,|10\rangle\langle 10| + a^*b\,|11\rangle\langle 00|\right) + (1-p)\dfrac{\mathbb{1}}{4}$

$$= p\,\underbrace{\begin{array}{cc} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} & \\ \begin{pmatrix} 0 & 0 & 0 & a^*b \\ 0 & |a|^2 & 0 & 0 \\ 0 & 0 & |b|^2 & 0 \\ ab^* & 0 & 0 & 0 \end{pmatrix} & \begin{array}{c} \langle 00| \\ \langle 01| \\ \langle 10| \\ \langle 11| \end{array} \end{array}}_{=:\,A} + (1-p)\frac{\mathbb{1}}{4}$$

- The spectrum of A is:

EIGENSTATE		EIGENVALUE
$\circ\ |01\rangle$	$\rightsquigarrow$	$|a|^2$
$\circ\ |10\rangle$	$\rightsquigarrow$	$|b|^2$

$$\tilde{A} := A\big|_{\{|00\rangle, |11\rangle\}} = \begin{pmatrix} 0 & a^*b \\ ab^* & 0 \end{pmatrix} \Rightarrow \det\left(\tilde{A} - \lambda\mathbb{1}\right) = \det\left[\begin{pmatrix} -\lambda & a^*b \\ ab^* & -\lambda \end{pmatrix}\right] = 0 \Rightarrow \lambda^2 - |a|^2|b|^2 = 0$$

$$\Rightarrow \lambda = \pm|a||b|$$

$$\hat{A}|v\rangle = \pm|a||b|\,|v\rangle \Longrightarrow \begin{pmatrix} \mp|a||b| & a^* b \\ a b^* & \mp|a||b| \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0 \Rightarrow$$

$$\Rightarrow y = \pm \frac{a b^*}{|a||b|} x \underset{\substack{\text{NORMALIZ.} \\ |x|^2+|y|^2=1}}{\Rightarrow} \begin{cases} |x|^2 + \frac{|a|^2|b|^2}{|a|^2|b|^2}|x|^2 = 1 \\ y = \pm \frac{a b^*}{|a||b|} x \end{cases}$$

$$\Rightarrow \begin{cases} x = \frac{1}{\sqrt{2}} e^{i\phi} \\ y = \pm \frac{a b^*}{|a||b|} \frac{1}{\sqrt{2}} e^{i\phi} \end{cases} \rightsquigarrow \begin{pmatrix} x \\ y \end{pmatrix} = \frac{e^{i\phi}}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm \frac{a b^*}{|a||b|} \end{pmatrix}$$

- The spectrum of A is:

EIGENSTATE		EIGENVALUE
$\|01\rangle$	$\rightsquigarrow$	$\|a\|^2$
$\|10\rangle$	$\rightsquigarrow$	$\|b\|^2$
$\frac{1}{\sqrt{2}}\left(\|00\rangle + \frac{a b^*}{\|a\|\|b\|}\|11\rangle\right)$	$\rightsquigarrow$	$\|a\|\|b\|$
$\frac{1}{\sqrt{2}}\left(\|00\rangle - \frac{a b^*}{\|a\|\|b\|}\|11\rangle\right)$	$\rightsquigarrow$	$-\|a\|\|b\|$

- The spectrum of $\rho_{(p)}^{T_B}$ is:

EIGENSTATE		EIGENVALUE	
$\|01\rangle$	$\rightsquigarrow$	$p\|a\|^2 + \frac{1}{4}(1-p)$	≥ 0
$\|10\rangle$	$\rightsquigarrow$	$p\|b\|^2 + \frac{1}{4}(1-p)$	≥ 0
$\frac{1}{\sqrt{2}}\left(\|00\rangle + \frac{a b^*}{\|a\|\|b\|}\|11\rangle\right)$	$\rightsquigarrow$	$p\|a\|\|b\| + \frac{1}{4}(1-p)$	≥ 0
$\frac{1}{\sqrt{2}}\left(\|00\rangle - \frac{a b^*}{\|a\|\|b\|}\|11\rangle\right)$	$\rightsquigarrow$	$-p\|a\|\|b\| + \frac{1}{4}(1-p)$	?

- $-p|a||b| + \frac{1}{4}(1-p) < 0 \iff p > \frac{1}{(1+4|a||b|)}$

- $p > \frac{1}{(1+4|a||b|)}$ $\Longleftrightarrow$ $\rho(p) := p\,|\psi\rangle\langle\psi| + (1-p)\frac{\mathbb{1}}{4}$. with $|\psi\rangle = a\,|01\rangle_{AB} + b\,|10\rangle_{AB}$ is entangled

e) Use the eigenvector corresponding to a negative eigenvalue of $(\rho(p))^{T_B}$ in order to derive an entanglement witness $\mathcal{W}$ for $\rho(p)$.

$p > \frac{1}{(1+4|a||b|)}$ $\Rightarrow$ $W := \left(|u\rangle\langle u|\right)^{T_B}$ with $|u\rangle := \frac{1}{\sqrt{2}}\left(|00\rangle - \frac{a\,b^*}{|a||b|}|11\rangle\right)$

$\frac{a\,b^*}{|a||b|} = 1$, if $a, b \in \mathbb{R}^+$.

is entangl. witness for $\rho(p)$.

(shown before)

f) Show that, in fact, the witness $\mathcal{W}$ detects *all* entangled states of the form $\rho(p)$.

$\forall\ p > \frac{1}{(1+4|a||b|)}$, $\rho(p)$ is entangled and

$$\mathrm{Tr}\left[W\,\rho(p)\right] = \mathrm{Tr}\left[|u\rangle\langle u|\,\rho^{T_B}(p)\right] \Rightarrow$$

$$= \langle u|\,\rho^{T_B}(p)\,|u\rangle < 0$$

$|u\rangle$ is eigenstate of $\rho^{T_B}(p)$ with eigenvalue < 0.

2. **Detecting Eve.** One key feature of the BB'84 protocol for quantum key distribution is that Alice and Bob are able to estimate how many bits were corrupted by the channel or Eve by comparing their results on a subset.

   In this excercise, we will prove this statement. More precisely, let Alice and Bob randomly select n of their $2n$ bits check for errors. We denote the number of errors in the test bits by e_T and the number of errors in the remaining, untested n bits by e_R. Then, for any $\delta > 0$

$$p := \Pr\{e_T \leq \delta n \ \wedge \ e_R \geq (\delta + \epsilon)\} \leq \exp\left[-\mathcal{O}(n\epsilon^2)\right]. \tag{1}$$

   In other words, the probability that the number of errors in the unknown bits deviatiates by more than ϵ from the observed fraction δ in the test bits gets very small large n and ϵ.

   We denote the total number of errors that occur in the $2n$ bits by μn.

   a) Argue that

$$p \leq \binom{2n}{n}^{-1} \binom{\mu n}{\delta n} \binom{(2-\mu)n}{(1-\delta)n} \delta n. \tag{2}$$

Solution: Ok, we are given a bit strings of length $2n$. This string can be partitioned into two strings of equal size in $\binom{2n}{n}$ ways. The number of ways in which we end up with one substring containing exactly i of the μn corrupted bits is $\binom{\mu n}{i}\binom{2n-\mu n}{n-i}$. Therefore, the probability of getting up to δn corrupted bits is

$$p = \binom{2n}{n}^{-1} \sum_{i=1}^{\delta n} \binom{\mu n}{i} \binom{(2-\mu)n}{n-i} \leq \binom{2n}{n}^{-1} \binom{\mu n}{\delta n} \binom{(2-\mu)n}{(1-\delta)n} \delta n, \tag{3}$$

where we have used that $i/n \leq \delta = \frac{\mu}{2} - \frac{\epsilon}{2} \leq \frac{\mu}{2}$.

We will need a few identities to massage this term. To this end, let $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ be the binary entropy.

b) Show that

$$nH(p) + \mathcal{O}(\log_2 n) \leq \log_2 \binom{n}{pn} \leq nH(p) + \mathcal{O}(\log_2 n). \tag{4}$$

Hint: Recall Stirling's bound $\sqrt{2\pi}\sqrt{n}\, n^n \mathrm{e}^{-n} \leq n! \leq \mathrm{e}\sqrt{n}\, n^n \mathrm{e}^{-n}$.

Solution: Setting $q = 1-p$,

$$\binom{n}{np} = \frac{n!}{(np)!(nq)!} \leq \frac{\mathrm{e}\sqrt{n}\,\left(\frac{n}{\mathrm{e}}\right)^n}{2\pi n\sqrt{pq}\,\left(\frac{np}{\mathrm{e}}\right)^{np}\left(\frac{nq}{\mathrm{e}}\right)^{nq}} \tag{5}$$

$$= \frac{\mathrm{e}}{2\pi\sqrt{npq}} p^{-np} q^{-nq}. \tag{6}$$

Taking the logarithm yields

$$\log_2 \binom{n}{np} \leq -n[p\log_2 p + q\log_2 q] + \log_2 \frac{e}{2\pi} - \frac{1}{2}\log_2 npq = nH(p) + \mathcal{O}(\log_2 n). \tag{7}$$

The lower bound follows analogously and only differs in the constant offset.

Furthermore, one can derive the following simple bound for the binary entropy $H(x) \leq 1 - 2\left(x - \frac{1}{2}\right)^2$. (If you are curious, it is a good excercise to use Taylor's theorem including an estimate for the remainder to derive this bound.)

Solution: The first derivatives of H are

$$H'(x) = -\log_2(x) + \log_2(1-x) \tag{8}$$

$$H''(x) = -\frac{1}{x\ln(2)} - \frac{1}{(1-x)\ln(2)} \tag{9}$$

$$H'''(x) = \frac{1}{x^2\ln(2)} - \frac{1}{(1-x)^2\ln(2)}. \tag{10}$$

The maximum of $H(x)$ is at $x_{\max} = \frac{1}{2}$ with $H(x_{\max}) = 1$ and $H''(x_{\max}) = -\frac{4}{\ln(2)} \geq 4$. Thus, by Taylor's theorem

$$H(x) = 1 - \frac{2}{\ln 2}\left(x - \frac{1}{2}\right)^2 + R(x) \leq 1 - 2\left(x - \frac{1}{2}\right)^2 + R(x), \tag{11}$$

with $R(x) = \frac{1}{6}H'''(\xi)\left(x - \frac{1}{2}\right)^3$ for suitable $\xi \in (\frac{1}{2}, x)$ for $x \geq \frac{1}{2}$ or $\xi \in (x, \frac{1}{2})$ for $x \leq \frac{1}{2}$. The third derivative can be written as $H'''(\xi) = -2\frac{\xi - \frac{1}{2}}{\xi^2\ln(2)(\xi-1)^2}$. Thus, as x and ξ are always on the same side of $\frac{1}{2}$ we always end up with an overall minus sign. So since $R(x) \leq 0$ for all x, it can be dropped to arrive at the bound.

c) Plug everything together and show that $p \leq \exp\left[-\mathcal{O}(n\epsilon^2)\right]$.

Solution: The solution of (b) implies that up to log-factors

$$\binom{bn}{an} \approx 2^{bnH(a/b)}. \tag{12}$$

Thus, up to log-terms in n

$$\log_2 p \leq -2nH(1/2) + \mu nH(\delta/\mu) + (2-\mu)nH\left(\frac{1-\delta}{2-\mu}\right) \tag{13}$$

$$\leq -2n + \mu n\left(1 - 2\left(\frac{\delta}{\mu} - \frac{1}{2}\right)^2\right) + (2-\mu)n\left(1 - 2\left(\frac{1-\delta}{2-\mu} - \frac{1}{2}\right)^2\right) \tag{14}$$

$$= -2n + \mu n - \frac{1}{2}\mu n(\epsilon/\mu)^2 + 2n - \mu n - \frac{1}{2}n\epsilon^2/(2-\mu) \tag{15}$$

$$= -\frac{1}{2}n\left(\frac{1}{\mu} + \frac{1}{2-\mu}\right)\epsilon^2 \tag{16}$$

$$= -n\frac{1}{\mu(\mu-2)}\epsilon^2 \in -\mathcal{O}(n\epsilon^2). \tag{17}$$

Here we have used that from $\delta = \mu/2 - \epsilon/2$ it follows that

$$2\left(\frac{\delta}{\mu} - \frac{1}{2}\right)^2 = \frac{1}{2}\left(\frac{\epsilon}{\mu}\right)^2 \tag{18}$$

and

$$2\left(\frac{1-\delta}{2-\mu} - \frac{1}{2}\right)^2 = \frac{1}{2}\left(\frac{2-\mu+\epsilon}{2-\mu} - 1\right)^2 \tag{19}$$

$$= -\frac{1}{2}\frac{\epsilon^2}{(2-\mu)^2}. \tag{20}$$