Freie Universität Berlin

Tutorials on Quantum Information Theory

Winter term 2022/23

Problem Sheet 8

Entanglement Witnesses and Cryptography

J. Eisert, A. Townsend-Teague, A. Mele, A. Burchards, J. Denzler

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., $\rho^{T_A} \geq 0$.

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.

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

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.

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 $\rho(p)^{T_B} \ngeq 0$.

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

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

[1] What is the corresponding noise channel for this model?

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

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

   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

$$nH(p) + \mathcal{O}(\log_2 n) \leq \log_2 \binom{n}{pn} \leq nH(p) + \mathcal{O}(\log_2 n). \tag{3}$$

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

   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.)

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