Quantum Cryptography (fall 2017)	Dominique Unruh
Exercise Sheet 6	
Out: 2017-11-03	Due: 2017-11-10

Problem 1: Trace Distance

(a) Let E_1 and E_2 be quantum ensembles. Let ρ_1 and ρ_2 be the corresponding density operators. Assume that E_1 and E_2 are physically indistinguishable. What is $\mathrm{TD}(\rho_1, \rho_2)$?

(b) Let $E_1 := \{(|+\rangle, \frac{1}{2}), (|-\rangle, \frac{1}{2})\}$ and $E_2 := \{(|0\rangle, 1)\}$ be quantum ensembles. Let ρ_1 and ρ_2 be the corresponding density operators. What is $\mathrm{TD}(\rho_1, \rho_2)$?

Note: You may use computer algebra software (e.g., SageMath) to compute the eigenvectors of matrices if you wish.

(c) Let $\rho = p\tau + q\rho'$ and $\sigma = p\tau + q\sigma'$ where τ, ρ', σ' are density operators, and $p, q \geq 0$, $p + q = 1$. Show that $\mathrm{TD}(\sigma, \rho) = q \cdot \mathrm{TD}(\sigma', \rho')$.

Note: Do not use Lemma 9 in the lecture notes.

(d) Let $E_1 := \{(|+\rangle, \frac{1}{4}), (|-\rangle, \frac{1}{4}), (|\Psi\rangle, \frac{1}{2})\}$. Let $E_2 := \{(|0\rangle, \frac{1}{2}), (|\Psi\rangle, \frac{1}{2})\}$. Here $|\Psi\rangle := \frac{1}{\sqrt{3}}|0\rangle - \sqrt{\frac{2}{3}}|1\rangle$. Let ρ_1 and ρ_2 be the corresponding density operators. What is $\mathrm{TD}(\rho_1, \rho_2)$?

Hint: Consider (c).

(e) Consider the following setup: Alice has a secret bit $b \in \{0, 1\}$. Then she chooses randomly $r \in \{0, 1\}$. If $r = 0$, she encodes b in the $|0\rangle, |1\rangle$ basis (i.e., she sends $|0\rangle$ for $b = 0$ and $|1\rangle$ for $b = 1$). If $r = 1$, she encodes b in the $|+\rangle, |-\rangle$ basis. Then she sends the resulting state $|\Psi_b\rangle$ to Eve. Show that the trace distance between the mixed states ρ_0 and ρ_1 corresponding to $b = 0$ and $b = 1$, respectively, is $\mathrm{TD}(\rho_0, \rho_1) = \frac{1}{\sqrt{2}}$.

Hint: The eigenvalues of $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$ are $\frac{1}{\sqrt{2}}$ and $-\frac{1}{\sqrt{2}}$. Note that this is not the toy protocol from the lecture, in the toy protocol b selected the basis, not r.

(f) In the experiment described in (e), assume that the bit b is chosen uniformly at random. Show that Eve cannot guess b with probability larger than $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 85\%$.

Hint: Try to express the probability that Eve guesses correctly in terms of $\Pr[G = x|b = y]$ for various $x, y \in \{0, 1\}$ (here G denotes Eve's guess) and then use (e).