Quantum Cryptography

# Homework Set 3

*Please send your answers – either typeset on a computer, or handwritten (but readable) and scanned, preferably in PDF format – to* `bouman@cwi.nl` *before April 4, 23h59. Do not forget to put your name on the first page. Good luck!*

## 1 The Partial Trace

a) Trace out the first part of the EPR state $|\Phi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big)$.

b) Show that $\mathrm{tr}_A(\rho_{AB}) \in \mathcal{D}(\mathcal{H}_B)$ for any density matrix $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

c) Show that for any composite quantum state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the density matrix obtained by tracing out $A$ coincides with the *expected* density matrix obtained by measuring $A$ in an arbitrary orthonormal basis $\mathcal{B} = \{|i\rangle\}_{i\in I}$ and "cutting off" (i.e., tracing out) the measured part. I.e., show that $\mathrm{tr}_A(\rho_{AB}) = \sum_{i\in I} p_i(\mathcal{B}\otimes\mathbf{I}, \rho_{AB})\mathrm{tr}_A(\rho_i(\mathcal{B}\otimes\mathbf{I}, \rho_{AB}))$.

## 2 Distance Between States

a) Argue that the trace norm $\|\cdot\|_{tr}$ is indeed a norm on the vector space of Hermitian matrices (of fixed dimension). *Hint:* Show and use that $\|A\|_{tr} = \max_E |\mathrm{tr}(EA)|$, where the max is over all Hermitian matrices $E$ with $\max_i |\lambda_i| \leq 1$, where $\{\lambda_i\}_i$ are the eigenvalues of $E$.

b) Show that for any two $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, there exists a basis $\mathcal{B}$ of $\mathcal{H}$ such that the respective probability distributions $P$ and $Q$, obtained by measuring the quantum states $\rho$ and $\sigma$ in basis $\mathcal{B}$, satisfy $\mathrm{SD}(P, Q) = \delta(\rho, \sigma)$.

c) Show that $\delta(\rho\otimes\tau, \sigma\otimes\tau) = \delta(\rho,\sigma)$, and that $\delta(U\rho U^\dagger, U\sigma U^\dagger) = \delta(\rho,\sigma)$ for arbitrary density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ and $\tau \in \mathcal{D}(\mathcal{H}')$ and any unitary matrix $U \in \mathcal{U}(\mathcal{H})$.

d) Show that $\delta(\rho,\sigma) \geq \delta\big(\mathrm{tr}_A(\rho), \mathrm{tr}_A(\sigma)\big)$ for any $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

## 3 Hybrid (Quantum-Classical) States

For the sake of brevity, we will write conditional operators like $\rho_{E|X=x}$ as $\rho_E^x$, i.e. we write the dependent variable in superscript and omit the associated random variable $X$.

We say that a composite state $\rho_{XE} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_E)$ is *classical on* $X$ if there exists an orthonormal basis $\{|x\rangle\}_{x\in\mathcal{X}}$ on $\mathcal{H}_X$ such that we can write $\rho_{XE}$ in the form $\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x$, where $P_X$ is a probability distribution and $\rho_E^x \in \mathcal{D}(\mathcal{H}_E)$ for every $x \in \mathcal{X}$.

a) Let $\rho_{XYE}$ have classical $X$ and $Y$, i.e.

$$\rho_{XYE} = \sum_{x,y} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^{x,y}.$$

Show that $\mathrm{tr}_X(\rho_{XYE}) = \sum_y P_Y(y)|y\rangle\langle y| \otimes \rho_E^y$, where

$$\rho_E^y = \sum_x P_{X|Y}(x|y)\rho_E^{x,y}$$

and $P_Y$ is naturally given by $P_Y(y) = \sum_x P_{XY}(x,y)$ for all $y$ and $P_{X|Y}(x|y)$ is naturally given by $P_{X|Y}(x|y) = P_{XY}(x,y)/P_Y(y)$ for all $y$ for which $P_Y(y) > 0$ and every $x$.

Let $\rho_{XE}$ be classical on $X$ with $\mathcal{X} = \{0,1\}$ and $P_X(0) = P_X(1) = \frac{1}{2}$. Think of system $X$ as your secret bit. System $E$ is held by Eve, whose task is to guess your bit $X$. Eve may apply an arbitrary measurement on her system $E$.

b) Find the probability with which she can guess $X$ correctly for the following choices of $\rho_E^x$ for every $x$:

1. $\rho_E^x = |x\rangle\langle x|$ 2. $\rho_E^x = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ 3. $\rho_E^x = \frac{1}{2}(|x\rangle\langle x| + H|x\rangle\langle x|H)$

## 4 Purification

Suppose that someone prepares a state of a quantum system $A$ according to the *ensemble* $\{(q_i, |\psi_i\rangle)\}_{i\in I}$, i.e. the $\{q_i\}_{i\in I}$ form a probability distribution, and the prepared state is equal to $|\psi_i\rangle$ with probability $q_i$.

a) Describe the prepared state as a density matrix $\rho_A$.

Let us introduce a system $R$ with $\mathcal{H}_R = \mathbb{C}^{|J|}$, and let $\mathcal{B} := \{|j\rangle\}_{j\in J}$ be an orthonormal basis for $\mathcal{H}_R$.

b) Construct a pure state $|\varphi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_R$, such that when measuring system $R$ of $|\varphi\rangle$ in basis $\mathcal{B}$ (and subsequently cutting off $R$) gives the ensemble that we started with, i.e. show that:

$$p_i(\mathbf{I} \otimes \mathcal{B}, |\varphi\rangle) = q_i \quad \text{and} \quad \mathrm{tr}_R(\rho_i(\mathbf{I} \otimes \mathcal{B}, |\varphi\rangle)) = |\psi_i\rangle$$

for all $i$.

c) Show that $\mathrm{tr}_R(|\varphi\rangle\langle\varphi|) = \rho_A$.