Quantum Cryptography

# Homework Set 3

*(Answer Sheet)*

## 1 The Partial Trace

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

**Answer:** For $\rho_{AB} = |\Phi\rangle\langle\Phi| = \frac{1}{2}\big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\big)$, the reduced density matrix equals

$$\begin{aligned}\mathrm{tr}_A(\rho_{AB}) &= \frac{1}{2}\big(\langle 0|0\rangle \otimes |0\rangle\langle 0| + \langle 0|1\rangle \otimes |0\rangle\langle 1| + \langle 1|0\rangle \otimes |1\rangle\langle 0| + \langle 1|1\rangle \otimes |1\rangle\langle 1|\big)\\ &= \frac{1}{2}\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big) = \frac{1}{2}\mathbb{I}\end{aligned}$$

which coincides with the density matrix obtained from the ensembles $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ or $\{(\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)\}$.

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

**Answer:** Due to linearity of the trace and due to convexity of $\mathcal{D}(\mathcal{H})$ (which is easy to see), it suffices to prove the claim for a pure state $\rho_{AB} = |\varphi\rangle\langle\varphi|$, where we may write $|\varphi\rangle = \sum_i \alpha_i |i\rangle|\psi_i\rangle$ for some orthonormal basis $\{|i\rangle\}_i$ (where $\langle\psi_i|\psi_i\rangle = 1$ and $\sum_i |\alpha_i|^2 = 1$). Then,

$$\mathrm{tr}_A(\rho) = \mathrm{tr}_A\Big(\sum_{i,j} \alpha_i \bar{\alpha}_j |i\rangle\langle j| \otimes |\psi_i\rangle\langle\psi_j|\Big) = \sum_i |\alpha_i|^2 |\psi_i\rangle\langle\psi_i|$$

which is in $\mathcal{D}(\mathcal{H}_B)$.

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 $\mathrm{tr}_A(\rho_{AB}) = \sum_{i\in I} p_i(\mathcal{B} \otimes \mathbf{I}, \rho_{AB})\mathrm{tr}_A(\rho_i(\mathcal{B} \otimes \mathbf{I}, \rho_{AB}))$.

**Answer:** By linearity of the two considered actions, it suffices to show the claim for a pure state $\rho_{AB} = |\varphi\rangle\langle\varphi|$. We can write $|\varphi\rangle = \sum_i \alpha_i |i\rangle|\psi_i\rangle$, where the $|i\rangle$'s form the considered basis. Then, $\mathrm{tr}_A(|\varphi\rangle\langle\varphi|) = \sum_{ij} \alpha_i \bar{\alpha}_j \mathrm{tr}_A(|i\rangle\langle j| \otimes |\psi_i\rangle\langle\psi_j|) = \sum_i |\alpha_i|^2 |\psi_i\rangle\langle\psi_i|$. On the other hand, measuring and cutting off $A$ results in the density matrix $|\psi_i\rangle\langle\psi_i|$ with probability $p_i = |\alpha_i|^2$, which on average equals $\sum_i |\alpha_i|^2 |\psi_i\rangle\langle\psi_i|$.

## 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 $E$.

**Answer:** The only non-trivial part is triangular inequality. By the claim on $\|\cdot\|_{tr}$, it follows that $\|A + B\|_{tr} = \max_E \big|\mathrm{tr}\big(E(A + B)\big)\big| \leq \max_E \big(|\mathrm{tr}(EA)| + |\mathrm{tr}(EB)|\big) \leq \|A\|_{tr} + \|B\|_{tr}$. It remains to prove the claim. The "$\leq$"-direction is rather clear, since we may assume without loss of generality $A$ to be in diagonal form (with its eigenvalues $\mu_i$ on the diagonal), and then we can choose $E$ in diagonal form as well with $\pm 1$ on the diagonal, depending on whether the corresponding eigenvalue of $A$ is positive or negative, so that $\mathrm{tr}(EA) = \sum_i |\mu_i| = \|A\|_{tr}$. For the other direction, consider again $A$ in diagonal form: $A = \big[\mu_1|1\rangle, \ldots, \mu_n|n\rangle\big]$, where $\{|1\rangle, \ldots, |n\rangle\}$ is the standard orthonormal basis. Then, for any Hermitian $E$ with $\max_i |\lambda_i| \leq 1$: $EA = \big[\mu_1 E|1\rangle, \ldots, \mu_n E|n\rangle\big]$, where (for any $i$) $E|i\rangle$ has Euclidean norm $\|E|i\rangle\|_2 \leq 1$, and thus in particular the $i$-th entry of $E|i\rangle$ is at most 1 in absolute value. It follows that $|\mathrm{tr}(EA)| \leq \sum_i |\mu_i| = \|A\|_{tr}$.

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 $\mathrm{SD}(P, Q) = \delta(\rho, \sigma)$.

**Answer:** Write $\rho - \sigma = \sum_j \lambda_j |j\rangle\langle j|$, where the $|j\rangle$'s are orthonormal eigenvectors of $\rho - \sigma$ (Spectral Decomposition Theorem). Then, $\delta(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_{tr} = \frac{1}{2}\sum_j |\lambda_j|$. On the other hand, the probabilities $p_i$ and $q_i$ to observe $i$ when measuring $\rho$ respectively $\sigma$ in basis $\{|i\rangle\}_i$ satisfy

$$p_i - q_i = \langle i|\rho|i\rangle - \langle i|\sigma|i\rangle = \langle i|(\rho - \sigma)|i\rangle = \sum_j \lambda_j \langle i||j\rangle\langle j||i\rangle = \lambda_i\,.$$

The statistical distance $\mathrm{SD}(P, Q) = \frac{1}{2}\sum_i |p_i - q_i| = \frac{1}{2}\sum_i |\lambda_i|$, and we see that this is equal to $\delta(\rho, \sigma)$.

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 $U\in\mathcal{U}(\mathcal{H})$.

**Answer:** The second claim is trivial, as such a unitary transformation does not change the eigenvalues of $\rho-\sigma$. The first claim is easy to see assuming that both $\rho-\sigma$ and $\tau$ are diagonal (with their eigenvalues on the diagonal), which we may do without loss of generality by the above.

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

**Answer:** We may write $\rho-\sigma$ as $\rho-\sigma=\sum_i\lambda_i|i\rangle\langle i|$, where the $\lambda_i$'s are the eigenvalues of $\rho-\sigma$ and the $|i\rangle$'s an orthonormal basis. Using linearity of the partial trace and triangle inequality, it follows that

$$\|\mathrm{tr}_A(\rho)-\mathrm{tr}_A(\sigma)\|_{tr}\leq\sum_i|\lambda_i|\|\mathrm{tr}_A(|i\rangle\langle i|)\|_{tr}=\sum_i|\lambda_i|=\|\rho-\sigma\|_{tr}$$

where we used that $\mathrm{tr}_A(|i\rangle\langle i|)\in\mathcal{D}(\mathcal{H}_B)$ and as such has trace norm 1.

## 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 $x$.

**Answer:**

$$\begin{aligned}\mathrm{tr}_X(\rho_{XYE})&=\mathrm{tr}_X\Big(\sum_{xy}P_{XY}(x,y)|x\rangle\langle x|\otimes|y\rangle\langle y|\otimes\rho_E^{x,y}\Big)\\&=\sum_{xy}P_{XY}(x,y)\mathrm{tr}_X(|x\rangle\langle x|\otimes|y\rangle\langle y|\otimes\rho_E^{x,y})\\&=\sum_y P_Y(y)|y\rangle\langle y|\otimes\sum_x P_{X|Y}(x|y)\rho_E^{x,y}\\&=\sum_y P_Y(y)|y\rangle\langle y|\otimes\rho_E^y.\end{aligned}$$

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

**Answer:** (1) Eve can measure $\rho_E^x$ in the computational basis and obtains $x$ correctly with probability 1. (2) $\rho_E^x$ is totally unrelated to $x$. Hence, Eve cannot do better than just guessing $x$, and this guess will be correct with probability 1/2. (3) Let $\rho_0=\frac{1}{2}(|0\rangle\langle 0|+|+\rangle\langle +|)$ and $\rho_1=\frac{1}{2}(|1\rangle\langle 1|+|-\rangle\langle -|)$. Recall that you have proved in 2b) that there always exists a measurement to *optimally* distinguish two states, i.e. so that $\delta(\rho_0,\rho_1)=\mathrm{SD}(p,q)$, where $p$ and $q$ are the probability distributions obtained when measuring $\rho_0$ and $\rho_1$ respectively. Eve constructs and uses this optimal measurement to measure her system $E$. We first compute the trace distance between $\rho_0$ and $\rho_1$:

$$\begin{aligned}\delta(\rho_0,\rho_1)&=\tfrac{1}{2}\mathrm{tr}|\tfrac{1}{2}(|0\rangle\langle 0|+|+\rangle\langle +|-|1\rangle\langle 1|-|-\rangle\langle -|)|=\tfrac{1}{2}\mathrm{tr}\left|\begin{pmatrix}1/2&1/2\\1/2&-1/2\end{pmatrix}\right|\\&=\tfrac{1}{2}\mathrm{tr}\sqrt{\begin{pmatrix}1/2&1/2\\1/2&-1/2\end{pmatrix}\begin{pmatrix}1/2&1/2\\1/2&-1/2\end{pmatrix}^\dagger}=\tfrac{1}{2}\mathrm{tr}\begin{pmatrix}\frac{1}{\sqrt{2}}&0\\0&\frac{1}{\sqrt{2}}\end{pmatrix}=1/\sqrt{2}.\end{aligned}$$

What remains is to connect the statistical distance to the guessing probability.

Let us write $p = (\frac{1}{2}-\alpha, \frac{1}{2}+\alpha)$ and $q = (\frac{1}{2}+\beta, \frac{1}{2}-\beta)$ for $\alpha, \beta \geq 0$. Then, the guessing probability is $\mathrm{Guess}(X|E) = P_X(0)\max_i p(i) + P_X(1)\max_j q(j) = \frac{1}{2}(\frac{1}{2}+\alpha) + \frac{1}{2}(\frac{1}{2}+\beta) = \frac{1}{2} + \frac{1}{2}(\alpha+\beta)$. Next, we compute $\mathrm{SD}(p,q)$ in terms of $\alpha$ and $\beta$:

$$\mathrm{SD}(p,q) = \tfrac{1}{2}\sum_i |p(i) - q(i)| = \alpha + \beta.$$

Hence,

$$\mathrm{Guess}(X|E) = \tfrac{1}{2} + \tfrac{1}{2}\mathrm{SD}(p,q) = \tfrac{1}{2} + \tfrac{1}{2}\delta(\rho_0,\rho_1) = \tfrac{1}{2} + \tfrac{1}{2\sqrt{2}} \approx .85.$$

## 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 $\rho_A$.

**Answer:**

$$\rho_A = \sum_{i\in I} q_i\, |\psi_i\rangle\langle\psi_i|.$$

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:

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

for all $i$.

**Answer:** We claim that $|\varphi\rangle = \sum_{i\in I}\sqrt{q_i}|\psi_i\rangle|i\rangle$ satisfies the required properties.

Indeed,

$$p_i(\mathbf{I}\otimes\mathcal{B}) = \langle\varphi|(\mathbb{I}_A\otimes|i\rangle\langle i|)|\varphi\rangle = (\sum_{j\in I}\sqrt{q_j}\langle\psi_j|\langle j|)(\mathbb{I}_A\otimes|i\rangle\langle i|)(\sum_{k\in I}\sqrt{q_k}|\psi_k\rangle|k\rangle)$$
$$= \sum_{j,k\in I}\sqrt{q_j q_k}\langle\psi_j|\psi_k\rangle\langle j|i\rangle\langle i|k\rangle = q_i,$$

and

$$\rho_i(\mathbf{I}\otimes\mathcal{B}, |\varphi\rangle) = \tfrac{1}{\sqrt{q_i}}(\mathbb{I}_A\otimes|i\rangle\langle i|)\sum_{j\in I}\sqrt{q_j}|\psi_j\rangle|j\rangle = |\psi_i\rangle|i\rangle.$$

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

**Answer:**

$$\mathrm{tr}_R(|\varphi\rangle\langle\varphi|) = \mathrm{tr}_R((\sum_{i\in I}\sqrt{q_i}|\psi_i\rangle|i\rangle)(\sum_{j\in I}\sqrt{q_j}\langle\psi_j|\langle j|))$$
$$= \mathrm{tr}_R(\sum_{i,j\in I}\sqrt{q_i q_j}|\psi_i\rangle\langle\psi_j|\otimes|i\rangle\langle j|)$$
$$= \sum_{i,j\in I}\langle i|j\rangle\sqrt{q_i q_j}|\psi_i\rangle\langle\psi_j| = \sum_{i\in I} q_i|\psi_i\rangle\langle\psi_i| = \rho_A.$$