Quantum Cryptography

Homework Set 1

(Answer Sheet)

We make use of the following notation. For any collection $\mathbf{M} = \{M_i\}_{i\in I}$ of measurement matrices that act on $\mathcal{H}$ and that satisfy $\sum_i M_i^\dagger M_i = \mathbb{I}$ and for any density matrix $\rho \in \mathcal{D}(\mathcal{H})$ we define

$$p_i(\mathbf{M}, \rho) := \mathrm{tr}(M_i^\dagger M_i \, \rho)$$

and

$$\rho_i(\mathbf{M}, \rho) := \frac{1}{p_i(\mathbf{M}, \rho)} M_i \rho M_i^\dagger$$

for all $i \in I$. Finally, we write $\mathbf{M_A} \otimes \mathbf{I_B}$ for the collection $\{M_{A,i} \otimes \mathbb{I}_B\}_{i\in I}$ of measurement matrices that act on $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathbf{M_A} = \{M_{A,i}\}_{i\in I}$ is a collection of measurement matrices that act on $\mathcal{H}_A$.

1 Unitary Evolution

a) Prove that for any $\rho \in \mathcal{D}(\mathcal{H})$ and $U \in \mathcal{U}(\mathcal{H})$: $U\rho U^\dagger \in \mathcal{D}(\mathcal{H})$.

Answer: By the invariance of the trace under a basis transformation (and since $U^\dagger = U^{-1}$ by definition of a unitary matrix): $\mathrm{tr}(U\rho U^\dagger) = \mathrm{tr}(\rho) = 1$. Furthermore, for any vector $|\psi\rangle \in \mathcal{H}$, setting $|\varphi\rangle = U|\psi\rangle$, it holds that $\langle\psi|U\rho U^\dagger|\psi\rangle = \langle\varphi|\rho|\varphi\rangle \geq 0$. Thus, $U\rho U^\dagger \in \mathcal{D}(\mathcal{H})$.

b) Show that for any unitary operator $U \in \mathcal{U}(\mathcal{H})$ and any quantum state $\rho \in \mathcal{D}(\mathcal{H})$, measuring $U\rho U^\dagger$ in basis $\mathcal{B} = \{|i\rangle\}_{i\in I}$ and measuring ρ in basis $U^\dagger\mathcal{B} = \{U^\dagger|i\rangle\}_{i\in I}$ produces the same probability distribution on the observed outcome.

Answer: Follows immediately from the observation that $p_i = \langle i|U\rho U^\dagger|i\rangle$ can be parsed as $p_i = \langle i|(U\rho U^\dagger)|i\rangle$ and as $p_i = (\langle i|U)\rho(U^\dagger|i\rangle)$, where $\langle i|U$ is the bra-vector corresponding to $U^\dagger|i\rangle$, i.e., $\langle i|U = (U^\dagger|i\rangle)^\dagger$.

2 Orthonormal Bases

Show that for any orthonormal basis $\{|i\rangle\}_{i\in I}$ of $\mathcal{H}$: $\sum_i |i\rangle\langle i| = \mathbb{I}$. Also show that if $\{|i\rangle\}_{i\in I}$ is an arbitrary basis of $\mathcal{H}$ with $\sum_i |i\rangle\langle i| = \mathbb{I}$, then it is an *orthonormal* basis.

Answer: Let $\{|i\rangle\}_{i\in I}$ be an arbitrary basis of $\mathcal{H}$. Consider the matrix $T = \sum_i |i\rangle\langle i| - \mathbb{I}$. For any $|j\rangle \in \{|i\rangle\}_{i\in I}$ it holds that

$$T|j\rangle = \sum_i |i\rangle\langle i| \cdot |j\rangle - |j\rangle = \sum_i |i\rangle\langle i|j\rangle - |j\rangle = \sum_{i\neq j} |i\rangle\langle i|j\rangle + |j\rangle(\langle j|j\rangle - 1)\,.$$

Thus, $T|j\rangle = 0$ for every basis vector $|j\rangle$ if and only if $\langle i|j\rangle = 0$ and $\langle j|j\rangle = 1$ for every $i \neq j \in I$, and thus if and only if $\{|i\rangle\}_{i\in I}$ is an *orthonormal* basis.

3 Composite Systems

a) Show that for any $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ and $\rho_B \in \mathcal{D}(\mathcal{H}_B)$: $\rho_A \otimes \rho_B \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

Answer: The trace sums the diagonal elements of a matrix. Let d_i be the ith diagonal element of ρ_A and let e_j be the jth diagonal element of ρ_B. Then $\mathrm{tr}(\rho_A \otimes \rho_B) = \sum_{ij} d_i e_j = (\sum_i d_i)(\sum_j e_j) = \mathrm{tr}(\rho_A) \cdot \mathrm{tr}(\rho_B) = 1$. Furthermore, we can always perform an eigendecomposition on a density matrix, and its positivity guarantees that the diagonal matrix in the decomposition will have non-negative diagonal entries. We write

$$\rho_A \otimes \rho_B = (U\Lambda U^\dagger) \otimes (U'\Lambda' U'^\dagger) = (U \otimes U')(\Lambda \otimes \Lambda')(U^\dagger \otimes U'^\dagger)$$

then, $U \otimes U'$ is unitary and $U^\dagger \otimes U'^\dagger$ is its adjoint. $\Lambda \otimes \Lambda'$ is a diagonal matrix with nonnegative values. Thus $\rho_A \otimes \rho_B$ is positive.

Consider a *product* state $\rho_{AB} = \rho_A \otimes \rho_B \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Assume that ρ_{AB} is measured by measurement operators that have product structure, i.e. $\mathbf{M_{AB}} = \{M_{ij}\}_{i\in I, j\in J}$ where $M_{ij} = M_{A,i} \otimes M_{B,j}$ for all $(i,j) \in I \times J$, and where $\mathbf{M_A} = \{M_{A,i}\}_{i\in I}$ and $\mathbf{M_B} = \{M_{B,j}\}_{j\in J}$ are collections of measurement operators on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively that both satisfy the completeness condition.

b) Show that $\mathbf{M_{AB}}$ satisfies the completeness condition, i.e. show that $\sum_{ij} M_{ij} = \mathbb{I}$.

Answer:
$\sum_{ij} M_{ij} = \sum_{ij} M_{A,i} \otimes M_{B,j} = (\sum_i M_{A,i}) \otimes (\sum_j M_{B,j}) = \mathbb{I}_A \otimes \mathbb{I}_B = \mathbb{I}_{AB}$.

c) Argue that the two observations are statistically independent for any choice of $\mathbf{M}_A$ and $\mathbf{M}_B$, and the two marginal distributions coincide with the respective distributions obtained when measuring the "single" quantum states ρ_A and ρ_B using respectively $\mathbf{M}_A$ and $\mathbf{M}_B$. I.e., show that $p_{ij}(\mathbf{M}_{AB}, \rho_{AB}) = p_i(\mathbf{M}_A, \rho_A) \cdot p_j(\mathbf{M}_B, \rho_B)$.

Answer: Since we are only interested in the outcome distribution, we use the POVM formalism and define $E_{ij} := M_{ij}^\dagger M_{ij}$, $E_{A,i} := M_{A,i}^\dagger M_{A,i}$ and likewise for $E_{B,j}$ for all i and j.

$$\begin{aligned} p_{ij}(\mathbf{M}, \rho_{AB}) &= \mathrm{tr}(E_{ij}\rho_{AB}) = \mathrm{tr}((E_{A,i} \otimes E_{B,j})(\rho_A \otimes \rho_B)) \\ &= \mathrm{tr}(E_{A,i}\rho_A \otimes E_{B,j}\rho_B) \\ &= \mathrm{tr}(E_{A,i}\rho_A)\mathrm{tr}(E_{B,j}\rho_B) = p_i(\mathbf{M}_A, \rho_A)p_j(\mathbf{M}_B, \rho_B) \end{aligned}$$

This is indeed the "product distribution" of the two distributions obtained by measuring the "single" quantum states ρ_A and ρ_B using respectively $\{M_{A,i}\}_{i\in I}$ and $\{M_{B,j}\}_{j\in J}$.

Consider a *composite state* $\sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

d) Argue that the result of measuring system A of σ_{AB} using $\mathbf{M}_A$ and B using $\mathbf{M}_B$ (in any order) is the same as when measuring σ_{AB} using the product measurement $\mathbf{M}_{AB}$. I.e., show that

$$p_{ij}(\mathbf{M}_{AB}, \sigma_{AB}) = p_i(\mathbf{M}_A \otimes \mathbf{I}_B, \sigma_{AB}) \cdot p_j(\mathbf{I} \otimes \mathbf{M}_B, \rho_i(\mathbf{M}_A \otimes \mathbf{I}_B, \sigma_{AB})).$$

Answer: To shorten notation, we use the POVM elements defined in the previous answer.

$$\begin{aligned} &p_i(\mathbf{M}_A \otimes \mathbf{I}_B, \sigma_{AB}) \cdot p_j(\mathbf{I}_A \otimes \mathbf{M}_B, \rho_i(\mathbf{M}_A \otimes \mathbf{I}_B, \sigma_{AB})) \\ &= \mathrm{tr}((E_{A,i} \otimes \mathbb{I}_B)\sigma_{AB}) \cdot \mathrm{tr}(\mathbb{I}_A \otimes E_{B,j} \frac{(M_{A,i} \otimes \mathbb{I}_B)\sigma_{AB}(M_{A,i} \otimes \mathbb{I}_B)^\dagger}{\mathrm{tr}((E_{A,i} \otimes \mathbb{I}_B)\sigma_{AB})}) \\ &= \mathrm{tr}((\mathbb{I}_A \otimes E_{B,j})(M_{A,i} \otimes \mathbb{I}_B)\sigma_{AB}(M_{A,i} \otimes \mathbb{I}_B)^\dagger) \\ &= \mathrm{tr}((M_{A,i} \otimes E_{B,j})\sigma_{AB}(M_{A,i}^\dagger \otimes \mathbb{I}_B)) \\ &= \mathrm{tr}((E_{A,i} \otimes E_{B,j})\sigma_{AB}) = \mathrm{tr}(E_{ij}\sigma_{AB}) = p_{ij}(\mathbf{M}_{AB}, \sigma_{AB}), \end{aligned}$$

where we have used the linearity and circularity of the trace to obtain respectively the second and the fourth equality.

e) Let $\mathcal{B}_A = \{|i\rangle\}_{i\in I}$ be an orthonormal basis of a system A, and let $\{U_i\}_{i\in I}$ be a family of unitary matrices acting on a system B. Show that $U = \sum_i |i\rangle\langle i| \otimes U_i$ is a unitary matrix, acting on the joint system AB. And, show that for any composite quantum state $|\varphi\rangle \in \mathcal{H}_{AB}$, measuring A in basis $\mathcal{B}_A$ to observe $i \in I$ and then applying the corresponding U_i to B gives the same state as when first applying U to $|\varphi\rangle$ and then measuring A.

Hint: use the state-vector formalism.

Answer: First, note that

$$U^\dagger U = \sum_{ij} |i\rangle\langle i||j\rangle\langle j| \otimes U_i^\dagger U_j = \sum_i |i\rangle\langle i| \otimes U_i^\dagger U_i = \sum_i |i\rangle\langle i| \otimes \mathbb{I}_B = \mathbb{I}_A \otimes \mathbb{I}_B = \mathbb{I}_{AB}$$

so that indeed U is unitary. Now, write $|\varphi\rangle$ as $|\varphi\rangle = \sum_i \alpha_i |i\rangle|\psi_i\rangle$ (with normalized $|\psi_i\rangle$'s). Thus, when first measuring $|\varphi\rangle$ in basis $\mathcal{B}_A$, then i is observed with probability $p_i = |\alpha_i|^2$ and the state of B collapses to $|\psi_i\rangle$, which is then transformed to $U_i|\psi_i\rangle$. On the other hand, if we first apply U to obtain

$$\begin{aligned} U|\varphi\rangle &= \Big(\sum_i |i\rangle\langle i| \otimes U_i\Big)\Big(\sum_j \alpha_j |j\rangle|\psi_j\rangle\Big) \\ &= \sum_{ij} \alpha_j |i\rangle\langle i||j\rangle \otimes U_i|\psi_j\rangle = \sum_i \alpha_i |i\rangle \otimes U_i|\psi_i\rangle \end{aligned}$$

then when measuring A in basis $\mathcal{B}_A$, outcome i is observed with the same probability $p_i = |\alpha_i|^2$ and the state collapses to $U_i|\psi_i\rangle$.

4 Measurement

a) Consider the qubit state $|\varphi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \in \mathbb{C}^2$. What are the probabilities to observe 0 and 1 when measuring $|\varphi\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$? What are the probabilities to observe the two possible outcomes, let's name them again 0 and 1, when measuring $|\varphi\rangle$ in the Hadamard basis $\{H|0\rangle, H|1\rangle\}$?

Answer: When measuring in the computational basis, one observes 0 and 1 with respective probabilities $p_0 = \left|\frac{1}{2}\right|^2 = \frac{1}{4}$ and $p_1 = \left|\frac{\sqrt{3}}{2}\right|^2 = \frac{3}{4}$. For the

measurement in the Hadamard basis, let's write $|\varphi\rangle$ as

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)\cdot\frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)+\frac{1}{\sqrt{2}}\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\right)\cdot\frac{1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)$$
$$= \frac{1}{\sqrt{2}}\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)H|0\rangle)+\frac{1}{\sqrt{2}}\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\right)\cdot H|1\rangle$$

so that we can read off the probabilities to observe 0 and 1 as

$$p_0 = \frac{1}{2}\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{2}+\frac{\sqrt{3}}{4} \approx 0.93 \quad \text{and} \quad p_1 = \frac{1}{2}\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{2}-\frac{\sqrt{3}}{4} \approx 0.067$$

respectively.

b) Show that two states that are described by *different* density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ can be distinguished with positive advantage by a suitable measurement. I.e., show that there exists some $\mathbf{M} = \{|j\rangle\langle j|\}_{j\in I}$ such that $p_i(\mathbf{M}, \rho) \neq p_i(\mathbf{M}, \sigma)$ for at least one $i \in I$.
Hint: Measure in a basis consisting of eigenvectors of $\rho - \sigma$.

Answer: Write $\rho - \sigma = \sum_{j\in I} \lambda_j |j\rangle\langle j|$, where the $|j\rangle$'s are orthonormal eigenvectors of $\rho - \sigma$ (Spectral Decomposition Theorem A.6). Now, we define $\mathbf{M} := \{|j\rangle\}_{j\in I}$ and write

$$p_i(\mathbf{M},\rho) - p_i(\mathbf{M},\sigma) = \langle i|\rho|i\rangle - \langle i|\sigma|i\rangle = \langle i|(\rho-\sigma)|i\rangle = \sum_j \lambda_j \langle i||j\rangle\langle j||i\rangle = \lambda_i\,.$$

Therefore, unless all λ_j's vanish, and thus $\rho = \sigma$, the two probability distributions are different, and thus can be distinguished with positive advantage.

5 Magic with an EPR Pair

An EPR pair is the two-qubit state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. Suppose that Alice holds (i.e., has control over) qubit A and Bob holds qubit B. Let $U \in \mathcal{U}(\mathbb{C}^2)$ be a unitary with real entries. Show that the following states are the same:

1. the state obtained if Alice applies U to her qubit of the EPR-pair;
2. the state obtained if Bob applies the transpose U^T (which coincides with $U^\dagger$ because U has real entries) to his qubit.

Answer: Applying U to Alice's qubit yields the state $\frac{1}{\sqrt{2}}(U|0\rangle\otimes|0\rangle + U|1\rangle\otimes|1\rangle)$. Applying U^T to Bob's qubit yields $\frac{1}{\sqrt{2}}(|0\rangle\otimes U^T|0\rangle + |1\rangle\otimes U^T|1\rangle)$. We now have to argue that these states are the same. We pre-multiply both states by $(\mathbb{I}\otimes U)$, which brings Bob's state back to the original EPR pair, and turns Alice's state into:

$$\frac{1}{\sqrt{2}}(U|0\rangle\otimes U|0\rangle + U|1\rangle\otimes U|1\rangle). \tag{1}$$

It remains to show that for a U with real entries, the above state is equal to the EPR pair. Because U is unitary, it preserves orthogonality. Hence, the following must hold for some real α and β:

$$U|0\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{and} \quad U|1\rangle = \pm(\beta|0\rangle - \alpha|1\rangle).$$

where $\alpha^2 + \beta^2 = 1$. We now substitute the relations above into (1):

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle+\beta|1\rangle)(\alpha|0\rangle+\beta|1\rangle) + (\beta|0\rangle-\alpha|1\rangle)(\beta|0\rangle-\alpha|1\rangle)$$
$$= \frac{1}{\sqrt{2}}((\alpha^2+\beta^2)|0\rangle|0\rangle + (\alpha^2+\beta^2)|1\rangle|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle).$$