Quantum Cryptography

Homework Set 1

Please send your answers – either typeset on a computer, or handwritten (but readable) and scanned, preferably in PDF format – to `bouman@cwi.nl` *before February 29, 23h59. Do not forget to put your name on the first page. Good luck!*

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 $U \in \mathcal{U}(\mathcal{H})$: $U \rho U^\dagger \in \mathcal{D}(\mathcal{H})$.

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.

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.

3 Composite Systems

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

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 $\sum_{ij} M_{ij} = \mathbb{I}$.

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 $p_{ij}(\mathbf{M}_{AB}, \rho_{AB}) = p_i(\mathbf{M}_A, \rho_A) \cdot p_j(\mathbf{M}_B, \rho_B)$.

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

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

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.

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 $\{H|0\rangle, H|1\rangle\}$?

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 $\rho - \sigma$.

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.