6.S895: Problem Set 1

Due: 23:59 March 8, 2024

1. **Entanglement practice (5pt)**

   (a) **(1pt)** Prove that $|\mathrm{EPR}\rangle\langle\mathrm{EPR}|$ is the only two-qubit mixed state where measuring both qubits in the X or Z basis yields the same outcome with certainty.

   (b) **(1pt)** The EPR state for d-dimensional qudits is $|\mathrm{EPR}_d\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle \otimes |i\rangle$. For any $d \times d$ matrix M, prove Ando's identity:

   $$(I \otimes M)\,|\mathrm{EPR}_d\rangle = (M^T \otimes I)\,|\mathrm{EPR}_d\rangle\,.$$

   Extra credit (0.1pts): who *was* Ando?

   (c) **(1pt)** The *Schmidt decomposition theorem* states that any bipartite pure state $|\Psi\rangle_{AB}$, it can be written as

   $$|\Psi\rangle_{AB} = \sum_{k=1}^{\ell} \alpha_k\,|u_k\rangle_A \otimes |v_k\rangle_B\,,$$

   where $\ell = \min(\dim(A), \dim(B))$, and the sets of vectors $\{|u_k\rangle\}$ and $\{|v_k\rangle\}$ are each orthonormal.

   Prove that if $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ both purify the same density matrix ρ_A, then they are related by a unitary on the B system:

   $$|\Psi\rangle_{AB} = (I \otimes U)\,|\Phi\rangle_{AB}\,.$$

   (d) **(1pt)** Show that if ρ_{AB} is a pure state then any purification $|\Psi\rangle_{ABE}$ can be written as a tensor product $|\Psi_1\rangle_{AB} \otimes |\Psi_2\rangle_E$.

   (e) **(1pt)** Prove that there is no three-qubit state $|\psi\rangle_{ABE}$ such that measuring ABE all in the X basis and all in the Z basis always yields the same outcome.

2. **Single-qubit quantum money schemes (16pt)**
   Consider the map $T : \mathrm{L}(\mathbb{C}^d) \to \mathrm{L}(\vee^n(\mathbb{C}^d))$ defined as follows:

   $$T(\rho) = P_{\mathrm{sym}}^{d,n}(\rho \otimes \mathrm{Id}_d^{\otimes m-1})P_{\mathrm{sym}}^{d,n} \tag{1}$$

   As a reminder, $\vee^n(\mathbb{C}^d)$ denotes the symmetric subspace on n qudits, $\mathrm{L}(\mathcal{H})$ for any Hilbert space $\mathcal{H}$ denotes the space of linear operators on $\mathcal{H}$ (density matrices live in this space), and $P_{\mathrm{sym}}^{d,n}$ denotes the projector onto the symmetric subspace in n qudits. In words, we can describe the action of T roughly as follows: T takes a single-qudit density matrix as input, adds some extra dimensions by tensoring with identity, and then projects into the symmetric subspace in the new n-qudit space.

(a) **(3pt)** Show that T is completely positive. (If you don't remember what this means, check Definition 2 of Lecture 1 from the lecture notes.)

(b) **(5pt)** Define a $\hat{T}$ with the same input and output spaces as T that is an appropriately normalised version of T which is a valid quantum channel, and show that $\hat{T}$ is a valid quantum channel.

(c) **(5pt)** For an ensemble consisting of the uniform distribution over k single-qubit states $|\psi_1\rangle, \ldots, |\psi_k\rangle$, define the success probability of any cloner C on this k-state ensemble to be

$$\frac{1}{k}\sum_{i=1}^{k} \mathrm{Tr}\Big[\big(|\psi_i\rangle \otimes |\psi_i\rangle\big)\big(\langle\psi_i| \otimes \langle\psi_i|\big)\, C(|\psi_i\rangle\langle\psi_i|)\Big]. \tag{2}$$

For instance, in class we studied this quantity for the Wiesner ensemble $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $k = 4$. Show that, for any single-qubit quantum money scheme drawing its states uniformly from a k-state ensemble for any k, there is a cloning attack which succeeds with probability at least $\frac{2}{3}$. (The optional part f of this problem shows that $\frac{2}{3}$ is tight: that is, there is a single-qubit money scheme where the best attack succeeds with probability at most $\frac{2}{3}$.)

(d) **(3pt)** Show that any single-qubit money scheme which draws its money states from an ensemble of only two pure states cannot be optimal (i.e. there is always an attack that succeeds with probability strictly better than $\frac{2}{3}$).

(e) **(optional, 0pt)** Think about whether this is true for three-state and four-state money ensembles over lunch, while taking a walk, or in the shower. Note: do NOT under any circumstances do all three at once.

(f) **(optional, 0pt)** In class, we showed that the optimal cloning probability for the single-qubit Wiesner scheme was $\frac{3}{4}$. Prove (using the same method or a different one) that the optimal cloning probability for the following six-state ensemble (where each state is chosen with $\frac{1}{6}$ probability)

$$\{|\psi_1\rangle = |0\rangle, |\psi_2\rangle = |1\rangle, |\psi_3\rangle = |+\rangle, |\psi_4\rangle = |-\rangle, |\psi_5\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}, |\psi_6\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}\} \tag{3}$$

is $\frac{2}{3}$, and therefore that this six-state ensemble improves over the Wiesner scheme. (It then follows from part (c) this six-state scheme is optimal.)

3. **Attacking the mutual information definition of QKD security (7pt)** In this problem we introduce a special notation for tensor products of Pauli matrices. First, label the Pauli matrices by

$$P_0 := I, P_1 := X, P_2 := Y, P_3 := Z.$$

Then for $y \in \{0, \ldots, 3\}^n$, we let P_y be the n-qubit tensor product operator

$$P_y = \bigotimes_{i=1}^{n} P_{y_i}.$$

(a) **(2pt)** For $x \in \{0, 1\}$ and $y \in \{0, \ldots, 3\}^n$, define the state

$$\rho_{AE} = \frac{1}{2^{2n+1}} \sum_{x\in\{0,1\}} \sum_{y\in\{0,\ldots,3\}^n} |xy\rangle\langle xy|_A \otimes \rho_E^{(x,y)},$$

where

$$\rho_E^{(x,y)} = \frac{1}{2^n}(I + (-1)^x P_y),$$

Prove that this is a valid quantum state. We will imagine that the A register is held by Alice and contains her $2n+1$-bit secret key, and the E register is held by Eve.

(b) **(2pt)** It can be shown that E has exponentially small mutual information with x, y: that is, any measurement on E will reveal exponentially little information about x and y. Now, suppose Alice measures her register to obtain a key x, y, and subsequently Eve learns y. Show that Eve can perform a measurement $\{M_{x'}^y\}$ on E whose outcome x' equals x with certainty. Intuitively, this means that learning $2n$ bits of information reveals $2n+1$ bits of information about the key.

(c) **(2pt)** Show that there exists a two-outcome measurement on the AE systems that, with advantage $1/2$, distinguishes ρ_{AE} from any state σ_{AE} of the form

$$\sigma_{AE} = \frac{1}{2^{2n+1}} \sum_{x,y} |xy\rangle \langle xy| \otimes \sigma_E,$$

where σ_E is any density matrix on the E system. Here "advantage" means that the difference in the probabilities that the measurement returns 0 for ρ_{AE} and σ_{AE} is $1/2$.

(d) **(1pt)** Argue that ρ_{AE} does not satisfy the security definition we gave in class, i.e. that for all states σ_E,

$$\|\rho_{AE} - \frac{1}{2^{2n+1}} \sum_{x,y} |xy\rangle \langle xy| \otimes \sigma_E\|_1 \geq c$$

for some constant c.