QUANTUM CRYPTOGRAPHY
Master of Logic, University of Amsterdam, 2017
TEACHERS: Jan Czajkowski, Yfke Dulek, and Christian Schaffner

Practice problem set 3

You do not have to hand in these exercises, they are for practicing only.

Problem 1: Min-entropy

What is the min-entropy of the following states?

(a) $\rho_X = |00\rangle\langle 00|$

(b) $\rho_X = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$

(c) $\rho_X = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$

(d) $\rho_X = \frac{3}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|$

(e) $\rho_X = \frac{1}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11| + \left(\frac{1}{4} - \epsilon\right)|01\rangle\langle 01| + \left(\frac{1}{4} + \epsilon\right)|10\rangle\langle 10|$

What is the conditional min-entropy of the following states? Is Eve ignorant about the key K?

(f) $\rho_{KE} = (|00\rangle_K|0\rangle_E)(\langle 00|_K\langle 0|_E)$

(g) $\rho_{KE} = \frac{1}{2}(|00\rangle_K|0\rangle_E)(\langle 00|_K\langle 0|_E) + \frac{1}{2}(|11\rangle_K|0\rangle_E)(\langle 11|_K\langle 0|_E)$

(h) $\rho_{KE} = \frac{3}{4}(|0\rangle_K|0\rangle_E)(\langle 0|_K\langle 0|_E) + \frac{1}{4}(|1\rangle_K|\circlearrowright\rangle_E)(\langle 1|_K\langle\circlearrowright|_E)$, where $|\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.

(i) Let K be a classical (key) register, and let E be Eve's quantum register. Prove the following statement for arbitrary classical-quantum states ρ_{KE}: Eve is ignorant about K if and only if $H_{min}(K|E) = \log|K|$.

Problem 2: Winning probability in the bipartite guessing game

Recall the bipartite guessing game: Eve prepares a state ρ_{AE}, and sends the A register to Alice. Alice chooses a random basis $\theta \in \{0,1\}$, and measures ρ_A in the computational basis if $\theta = 0$ or in the Hadamard basis if $\theta = 1$. She records the outcome X. Eve has to guess X, based on her state ρ_E and on θ. She wins if she guesses correctly.

(a) If ρ_E is has zero dimension (that is, Eve is not allowed to hold back any information), what is the maximum winning probability for Eve? What state ρ_A should she prepare?

(b) If ρ_E is has higher dimension (that is, Eve is allowed to keep an entangled state), what is the maximum winning probability for Eve? What state ρ_{AE} should she prepare?

Problem 3: Trace distance

Let $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ denote the EPR state. Alice and Bob try to create a shared EPR pair: $\rho_{\text{ideal}} = |\Phi\rangle\langle\Phi|$. Sadly, they are not very good at this yet and instead they create the shared state $\rho_{\text{real}} = (1-p)|\Phi\rangle\langle\Phi| + p\frac{\mathbb{I}}{4}$. What is the trace distance between ρ_{ideal} and ρ_{real}?

Problem 4: Guessing with three bases

Eve prepares a single-qubit state $|\psi\rangle$ and sends it to Alice. Alice then generates a random number $\theta \in \{0,1,2\}$. If $\theta = 0$ she measures in the standard basis (Z-basis), if $\theta = 1$ she measures in the Hadamard basis (X-basis), and if $\theta = 2$ she measures in the rotation basis (Y-basis). Alice announces θ to Eve, but not her measurement outcome x. Eve's goal is now to guess x.

(a) What is Eve's winning probability if $|\psi\rangle = |0\rangle$? What about $|\psi\rangle = |+\rangle$?

(b) In the guessing game with two bases, the state that gives Eve the optimal winning probability is $|\psi\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|0\rangle + |+\rangle)$. What is Eve's winning probability when using this state?

(c) What do you think the optimal $|\psi\rangle$ looks like for the three-bases guessing game? Is Eve's winning probability lower, equal, or higher than the optimal winning probability in the two-bases game?