Chair for Theoretical Information Technology
RWTH AACHEN UNIVERSITY

Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 4

Friday, May 10, 2019

Problem 1. *(Properties of entropy)*

Let X, Y be random variables with support $\mathcal{X} = \{x_1, \ldots, x_m\}$ and $\mathcal{Y} = \{y_1, \ldots, y_d\}$. Assume that X, Y are distributed by $P(X = x_i) = p_i$ and $P(Y = y_j) = q_j$. Let (X, Y) be the corresponding two-dimensional random variable with distribution $P(X = x_i, Y = y_j) = p_{ij}$. Prove the following statements from Theorem 4.3:

(a) $0 \leq H(X)$ with equality if and only if $P(X = x_i) = 1$ for some i.

(b) $H(X) \leq \log m$ with equality if and only if $P(X = x_i) = \frac{1}{m}$ for all i.

(c) $H(X \mid Y) \leq H(X)$ with equality if and only if X and Y are stochastically independent (conditioning reduces entropy).

(d) $H(X, Y) = H(X) + H(Y \mid X)$ (chainrule of entropies).

(e) $H(X, Y) \leq H(X) + H(Y)$ with equality iff X and Y are stochastically independent.

Hint (a): $\ln z \leq z - 1$ for all $z > 0$ with equality if and only if $z = 1$.

Hint (b), (c): If f is a convex function, the Jensen inequality $f(E(X)) \leq E(f(X))$ holds.

Problem 2. *(Entropy of function)* Let X, Y be discrete random variables on a set Ω. Show that for any function $f : X(\Omega) \times Y(\Omega) \to \mathbb{R}$, it holds

$$H(X, Y, f(X, Y)) = H(X, Y).$$

Problem 3. *(Proof Shannon's Theorem 4.13 on Perfect Secrecy)* Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem. Suppose that $P(\hat{M} = M) > 0$ for all $M \in \mathcal{M}$, $P(\hat{K} = K) > 0$ for all $K \in \mathcal{K}$ and $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ holds. Show that if $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ has perfect secrecy, then

$$P(\hat{K} = K) = \frac{1}{|\mathcal{K}|} \text{ for all } K \in \mathcal{K}$$

and for all $M \in \mathcal{M}, C \in \mathcal{C}$, there is a unique $K \in \mathcal{K}$ such that $e(M, K) = C$.