Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 4

Friday, May 13, 2016

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 and key equivocation)* Let $\mathcal{M} = \{a, b\}$ be the message space, $\mathcal{K} = \{K_1, K_2, K_3\}$ the key space and $\mathcal{C} = \{1, 2, 3, 4\}$ the ciphertext space. Let $\hat{M}, \hat{K}$ be stochastically independent random variables with support $\mathcal{M}$ and $\mathcal{K}$, respectively, and with probability distributions:

$$P(\hat{M} = a) = \frac{1}{4},\ P(\hat{M} = b) = \frac{3}{4},\ P(\hat{K} = K_1) = \frac{1}{2},\ P(\hat{K} = K_2) = \frac{1}{4},\ P(\hat{K} = K_3) = \frac{1}{4}.$$

The following table explains the encryption rules:

	K_1	K_2	K_3
a	1	2	3
b	2	3	4

, e.g., $e(a, K_1) = 1$.

a) Compute the entropies $H(\hat{M}), H(\hat{K}), H(\hat{C})$ and the key equivocation $H(\hat{K} \mid \hat{C})$.

b) Why does this cryptosystem not have perfect secrecy?

Problem 3. *(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 4. We have a cryptosystem with only two possible plaintexts. The plaintext a occurs with probability $1/3$ and b with probability $2/3$. There are two keys, k_1 and k_2, and each is used with probability $1/2$. Key k_1 encripts a to A and b to B. Key k_2 encripts a to B and b to A.

a) Calculate the entropy of the plaintext, $H(M)$.

b) Show that a Vernam Cipher with $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ has perfect secrecy. Indicate one disadvantage of the Vernam Cipher.

c) Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem with perfect secrecy. Show that:

$$H(C, M) = H(C) + H(M)$$

d) Let $\tilde{H}(Y|X) = -\sum_{x,y} p_Y(y|x)\, log_2\, p_Y(y|x)$. We assume X and Y to be discrete random variables. Show that if X and Y are independent, and X has $|\mathcal{X}| \geq 0$ possible outputs, then $\tilde{H}(Y|X) = |\mathcal{X}| \cdot H(Y) \geq H(Y)$.