UM. Autumn 2019. Homework 5 to the course «Information theory».
[not counted in *contrôle continu*]

Problem 1. Let (α, β, γ) be a triple of jointly distributed random variables. For every value c_k of γ we have a conditional distribution of probabilities of the values (α, β) (conditional on $\gamma = c_k$), $p_{ij} = \text{Prob}[\alpha = a_i \ \& \ \beta = b_j \,|\, \gamma = c_k]$. For this conditional distribution we can compute the mutual information between α and β; we denote this quantity $I(\alpha : \beta \,|\, \gamma = c_k)$.

The *conditional mutual information* between α and β given γ is defined as

$$I(\alpha : \beta \,|\, \gamma) := \sum_k \text{Prob}[\gamma = c_k] \cdot I(\alpha : \beta \,|\, \gamma = c_k)$$

Prove that

$$\begin{aligned} I(\alpha : \beta \,|\, \gamma) &= H(\beta \,|\, \gamma) - H(\beta \,|\, \alpha, \gamma) \\ &= H(\alpha \,|\, \gamma) - H(\alpha \,|\, \beta, \gamma) \\ &= H(\alpha \,|\, \gamma) + H(\beta \,|\, \gamma) - H(\alpha, \beta \,|\, \gamma) \\ &= H(\alpha, \gamma) + H(\beta, \gamma) - H(\alpha, \beta, \gamma) - H(\gamma). \end{aligned}$$

Problem 2. (a) Prove that $H(\alpha \,|\, \beta) = 0$ if and only if α is a deterministic function of β (every value of β is compatible with only one value of α).

(b) Prove that $I(\alpha : \beta) = H(\alpha)$ if and only if α is a deterministic function of β.

Problem 3. Prove that for all jointly distributed α, β, γ

$$I(\alpha : \langle \beta, \gamma \rangle) = I(\alpha : \beta) + I(\alpha : \gamma \,|\, \beta).$$

Problem 4. (a) Find an example of jointly distributed random variables α, β, γ such that $I(\alpha : \beta) < I(\alpha : \beta \,|\, \gamma)$.

(b) Find an example of jointly distributed α, β, γ such that

$$I(\alpha : \beta) > I(\alpha : \beta \,|\, \gamma).$$

Problem 5. (a) Prove that for all jointly distributed α, β, γ

$$I(\alpha : \beta) \le I(\alpha : \beta \,|\, \gamma) + H(\gamma).$$

(b) Prove that for all jointly distributed α, β, γ

$$I(\alpha : \beta \,|\, \gamma) \le I(\alpha : \beta) + H(\gamma).$$

Problem 6. Two random variables α and β are distributed on the set $\{1, \ldots, n\}$. Denote $\epsilon := \text{Prob}[\alpha \ne \beta]$. Prove that

$$H(\beta \,|\, \alpha) \le 1 + \epsilon \cdot \log(n - 1).$$

Problem 7. The sequence of random variables $\alpha \to \beta \to \gamma$ is a *Markov chain*, i.e., α and γ are independent conditional on β. Prove that

$$I(\alpha : \gamma) \leq I(\alpha : \beta)$$

and

$$I(\alpha : \gamma) \leq I(\beta : \gamma).$$

Problem 8. Let t, n be positive integer numbers ($t < n$), and $(S_0, S_1, \ldots, S_n)$ be a distribution such that

$$\text{(i) } H(S_0 \,|\, S_{i_1}, \ldots S_{i_t}) = 0$$

and for all $1 < i_1 < \ldots < i_t < n$, and

$$\text{(ii) } H(S_0 \,|\, S_{j_1}, \ldots S_{j_{t-1}}) = H(S_0)$$

for all $j_1, \ldots, j_{t-1}$ (a *secret sharing scheme* with the threshold t). Prove that $H(S_i) \geq H(S_0)$ for every $i = 1, \ldots, n$.

Remark : the proof should work for *all* secret sharing schemes with the threshold t, not only for Shamir's scheme discussed in the class.

Problem 9. Let $\epsilon \in (0, 1)$. It is known that some binary random variables α, β satisfy the conditions

$$\begin{aligned}
\text{Prob}[\beta = 0 \,|\, \alpha = 0] &= 1 - \epsilon, \\
\text{Prob}[\beta = 1 \,|\, \alpha = 1] &= 1 - \epsilon, \\
\text{Prob}[\beta = 0 \,|\, \alpha = 1] &= \epsilon, \\
\text{Prob}[\beta = 1 \,|\, \alpha = 0] &= \epsilon.
\end{aligned}$$

In other words, α is a bit with some (unknown) distribution, and β is obtained from α by flipping it with probability ϵ. Find the maximal possible value of $I(\alpha : \beta)$.

Problem 10. We toss a "fair" coin $N = 10^6$ times ; each throwing gives "heads" or "tails" with equal probabilities, and all N iterations are independent. Prove that

$$\text{Prob}\big[0.49 < [\text{fraction of "tails" among } N \text{ obtained results}] < 0.51\big] > 0.99.$$

Problem 11. (a) Prove that

$$1 + \sqrt{2} + \ldots + \sqrt{n} = an\sqrt{n} + b\sqrt{n} + O(1)$$

for some constants a, b.

(b) Find the values of a and b in this formula.

(c) Prove a similar formula for the sum $1 + \sqrt[3]{2} + \ldots + \sqrt[3]{n}$.