UM. Autumn 2020. Homework 5 to the course «Information theory».
[not counted in *contrôle continu*]

Problem 1. We are given $n = 5$ coins. One of them is fake, and can be lighter or heavier than all other (identical) coins. We can use balance scales to compare weights of any two groups of coins. We are not obliged to find out the relative weight of the fake coin (we ignore whether it is lighter or heavier than a genuine one). How many operations do we need to find the fake coin ?

Problem 2. Construct an optimal prefix code for the probability distribution

$$(0.4, 0.3, 0.15, 0.1, 0.5).$$

What is the average length of the codewords in this code (for the given distribution) ?

Problem 3. Construct an optimal prefix code for the probability distribution

$$\left(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{64}, \frac{1}{64}\right).$$

Find for this distribution a prefix code with the minimal possible average length of codewords. Compute the average length of codewords in this code.

Problem 4. 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

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

Problem 5. Let α be a random variables with a range $\{x_1, \dots, x_k\}$, and assume that $0 \le x_i \le 10$ for each i. Can we claim for this random variable that

(a) $0 \le E(\alpha) \le 10$?

(b) $\mathrm{var}(\alpha) \le 10^2$?

(c) $\mathrm{var}(\alpha) \le 5^2$?

(For each question, prove the inequality or find a counterexample.)

Problem 6. Let α be a random variable distributed on the set $\{x_1, \dots, x_{10^6}\}$.
(a) Is it possible that $H(\alpha) < 2$?
(b) Is it possible that $H(\alpha) < 1$?
(c) Is it possible that $H(\alpha) > 10$?
(d) Is it possible that $H(\alpha) > 20$?

Problem 7. Let α be a random variable distributed on the set $\{x_1, \dots, x_{10^6}\}$. It is known that $\mathrm{Prob}[\alpha = x_1] \ge 0.9$.
(a) Is it possible that $H(\alpha) > 1$?
(b) Is it possible that $H(\alpha) > 2$?
(c) Is it possible that $H(\alpha) > 10$?
(d) Is it possible that $H(\alpha) > 20$?

Problem 8. Prove that $H(\alpha \,|\, \alpha) = 0$ for all random variables α.

Problem 9. Prove that for all jointly distributed (α, β, γ)
(a) $H(\alpha, \beta \,|\, \gamma) \leq H(\alpha \,|\, \gamma) + H(\beta \,|\, \gamma)$,
(b) $H(\alpha, \beta, \gamma) + H(\gamma) \leq H(\alpha, \gamma) + H(\beta, \gamma)$.

Problem 10. Extend the definition of the conditional entropy to the case when the condition consists of several (jointly distributed) random variables and define the value of $H(\alpha|\beta, \gamma)$. Prove that for all jointly distributed (α, β, γ)

$$H(\alpha \,|\, \beta, \gamma) \leq H(\alpha \,|\, \beta).$$

Problem 11. Prove that for all jointly distributed (α, β, γ)

$$H(\alpha, \beta, \gamma) \leq H(\alpha) + H(\beta \,|\, \alpha) + H(\gamma \,|\, \beta).$$

Problem 12. Prove that for all jointly distributed $(\alpha_1, \ldots, \alpha_n)$

$$H(\alpha_1, \ldots, \alpha_n) \leq H(\alpha_1, \alpha_2) + H(\alpha_3 \,|\, \alpha_1, \alpha_2) + H(\alpha_4 \,|\, \alpha_2, \alpha_3) + \ldots + H(\alpha_n \,|\, \alpha_{n-2}, \alpha_{n-1}).$$

Problem 13. (a) Construct a joint distribution (α, β) such that for some a_i with a positive probability (i.e., $\mathrm{Prob}[\alpha = a_i] > 0$) we have

$$H(\beta \,|\, \alpha = a_i) > H(\beta).$$

(b) Prove that for every joint distribution (α, β) there is at least one value a_i with a positive probability (i.e., $\mathrm{Prob}[\alpha = a_i] > 0$) such that

$$H(\beta \,|\, \alpha = a_i) \leq H(\beta).$$

Problem 14. Two random variables α and β are distributed on the set $\{1, \ldots, k\}$. Denote $\epsilon := \mathrm{Prob}[\alpha \neq \beta]$.
(a) Prove that $H(\beta \,|\, \alpha) \leq 1 + \epsilon \cdot \log k$.
(b) Prove that $H(\beta \,|\, \alpha) \leq 1 + \epsilon \cdot \log(k - 1)$.

Problem 15. Construct a pair of jointly distributed random variables (α, β) such that $\mathrm{Prob}[\alpha \neq \beta] < 1/100$ but $H(\alpha \,|\, \beta) > 100$.

Problem 16. Prove that $H(\alpha \,|\, \beta) = 0$ only if α is a deterministic function of β (every value of β is compatible with only one value of α).

Problem 17. Two random variables α and β are distributed on the set $\{1, \ldots, k\}$. It is known $\mathrm{Prob}[\alpha = \beta] = 0$.

(a) Is it possible that $H(\alpha \,|\, \beta) = 0$?

(a) Is it possible that $H(\alpha \,|\, \beta) = 0$ and $H(\beta \,|\, \alpha) = 0$?

Problem 18. Two random variables α and β are distributed on the set $\{1, \ldots, k\}$ and $\mathrm{Prob}[\alpha \neq \beta] = 0.99$. Prove that

$$H(\beta) \leq H(\alpha) + 0.01 \cdot \log k + 1.$$

Problem 19. Let α be a random variable with a range A of N elements. Assume also that there are functions

$$\begin{array}{rcccc} C & : & A & \to & \{0,1\}^k, \\ D & : & \{0,1\}^k & \to & A \end{array}$$

such that for a w in A randomly chosen with the distribution α

$$\mathrm{Prob}(D(C(w)) \neq w) = \epsilon.$$

Prove that $k \geq H(\alpha) - \epsilon \cdot \log N - 1$.

Problem 20. Let $\alpha_1, \ldots, \alpha_n$ be a sequence of independent identically distributed random variables, and let $h < H(\alpha_i)$. Denote A the range (the alphabet) of all α_i and $k(n) := \lceil hn \rceil$. Then for all pairs of functions (encoding and decoding)

$$\begin{array}{rcccc} C_n & : & A^n & \to & \{0,1\}^{k(n)}, \\ D_n & : & \{0,1\}^{k(n)} & \to & A^n \end{array}$$

the error probability

$$\epsilon_n := \mathrm{Prob}_{(\alpha_1 \ldots \alpha_n)} \left[D_n(C_n(w_1 \ldots w_n)) \neq w_1 \ldots w_n \right]$$

does *not* tends to 0 as $n \to \infty$. (Here the n-letter words $w_1 \ldots w_n$ is a randomly value of the sequence of random variables $(\alpha_1, \ldots, \alpha_n)$. In other words, each letter w_j is chosen with the distribution α_j, independently of other letters.)

Problem 21. Alice sends to Bob a random message α that has a distribution with an entropy $H(\alpha)$. To keep the message in secret from the eavesdropper, Alice encrypts α using a unique secret key γ,

$$\textbf{message} = \mathrm{EncriptionFunction}(\alpha, \gamma).$$

(The value of γ is known in advance to Alice and to Bob, but not to the potential eavesdropper ; for every communication session Alice and Bob use a fresh value of γ). We say that EncriptionFunction is perfect, if

$$H(\alpha) = H(\alpha \,|\, \textbf{message})$$

that is, the eavesdropper who intercepts **message** gets *no* new information on the original secret text α. Prove that a perfect encoding scheme can exist only if $H(\gamma) \geq H(\alpha)$.

Slightly informally this fact can be phrased as follows : in a reliable encryption scheme, the size of the secret key must be at least as long as the size of the text to be encrypted.