UM. Autumn 2020. Homework to the course «Information theory» (not counted in *contrôle continu*).
[should be returned by Dec 22 to be corrected]

Problem 1. Assume that we have a joint distribution of random variables (S_0, S_1, S_2, S_3) such that

$$\begin{cases} H(S_0|S_1, S_2) = H(S_0), \\ H(S_0|S_1, S_2, S_3) = 0. \end{cases}$$

Prove that $H(S_3) \geq H(S_0)$.

(In some sense, this exercise explains that the secret sharing scheme discussed in the class cannot be improved : we cannot make the entropies of the "shares" smaller than the size of the secret S_0.)

Problem 2. (a) Prove that there exists a constant d_1 such that for all $x, y \in \{0,1\}^*$

$$C(x|y) \leq C(x) + d_1.$$

(b) Prove that there exists a constant d_2 such that for all $x \in \{0,1\}^*$

$$C(x|x) \leq d_2.$$

Problem 3. (a) Prove that for every computable function f there exists a constant d_f such that

$$C(f(x)) \leq C(x) + d_f.$$

(b) Prove that for every computable function g there exists a constant d_g such that

$$C(g(x)|x) \leq d_g.$$

Problem 4. A word $x \in \{0,1\}^n$ is a *palindrome* if x reads the same backward as forward, such as, for example, 11, 00100, 101101. Prove that there exists a constant d such that $C(x) \leq |x|/2 + d$.

Problem 5. In what follows xy denotes the concatenation of x and y.
(a) Prove that there exists a constant d_1 such that for all $x, y \in \{0,1\}^*$

$$C(xy) \leq 2C(x) + C(y) + d_1.$$

(b) Prove that there exists a constant d_2 such that for all $x, y \in \{0,1\}^*$

$$C(xy) \leq C(x) + C(y) + 2\log C(x) + d_2.$$

(c) Prove that there exists a constant d_3 such that for all $x, y \in \{0,1\}^*$

$$C(xy) \leq C(x) + C(y) + \log C(x) + \log\log C(x) + 2\log\log\log C(x) + d_3.$$

(d) Prove that there exists a constant d_4 such that for all $x, y \in \{0,1\}^*$

$$C(xy) \leq C(x) + C(y|x) + \log C(x) + \log\log C(x) + 2\log\log\log C(x) + d_4.$$

Problem 6. (a) Prove that for all n, d there are less than 2^{n-d} strings $x \in \{0,1\}^n$ such that $C(x) < n - d$.
(b) Prove that there exists a constant d such that for every n, for at least 99,9% of $x \in \{0,1\}^n$

$$n - d \leq C(x) \leq n + d.$$

Problem 7 (optional)**.** (a) Prove that for all real numbers a, b

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + b^{n-1}).$$

(b) Let $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial of degree n. Let x_0 be a root of this polynomial, i.e., $P(x_0) = 0$. Prove that there exists a polynomial $Q(x)$ such that $P(x) = (x - x_0)Q(x)$.
Hint : observe that

$$\begin{aligned} P(x) &= P(x) - 0 = P(x) - P(x_0) \\ &= a_0 + a_1x + a_2x^2 + \ldots + a_nx^n - (a_0 + a_1x_0 + a_2x^2 + \ldots + a_nx_0^n) \\ &= (a_0 - a_0) + a_1(x - x_0) + a_2(x^2 - x_0^2) + \ldots + a_n(x^n - x_0^n) \end{aligned}$$

and use (a).
(c) Let $P(x) = (x - x_1)Q(x)$ be a polynomial, and let x_2 ($x_2 \neq x_1$) be another root of $P(x)$. Prove that x_2 is also a root of $Q(x)$.
(d) Let $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial of degree n. Let $x_1, \ldots, x_n$ be (pairwise different) roots of this polynomial. Prove that

$$P(x) = a_n(x - x_0) \cdot (x - x_1) \cdot \ldots \cdot (x - x_n).$$

(e) Prove that a polynomial of degree n cannot have more than n pairwise different real roots.
(f) Let p be a prime number and $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial of degree n with integer coefficients (and a_n is not divisible by p). Prove that there exist at most n pairwise different numbers $x_i \in \{0, 1, \ldots, p-1\}$ such that

$$P(x_i) = 0 \mod p.$$

Hint : Reformulate and prove (a)-(d) in the arithmetic modulo p.
(g) Find a polynomial $P(x)$ of degree 2 with integer coefficients that has exactly *three* different roots modulo 6 (i.e., there are three pairwise different numbers x_1, x_2, x_3 in $\{0, 1, \ldots, 5\}$ such that $P(x_i) = 0 \mod 6$ for $i = 1, 2, 3$).