NIE-AIB — Homework 3 – 1.11.2023

Instructions.

Complete the exercises and write your solutions on papers. Comment your solutions sufficiently. **A result alone without the solution is insufficient**. Submit your solutions to the MS Teams assignment "NIE-AIB, Homework 3" no later than November 14.

1 Exercise 1.

Consider the polynomial $g(x) = x^3 + x + 1$. Show that there is a cyclic code C of length 8 over F_3 such that $g(x)$ is its generator polynomial. Find the generator polynomial of the code $C^\perp$.

2 Exercise 2.

Determine whether the following codes are linear and also whether they are cyclic. Briefly explain your answers.

- The ternary code $C = \left\{x \mid x \in F_3^5 \wedge w(x) = 0 \ (\mod 3)\right\}$.
- The 7-ary code $C = \left\{x \mid x \in F_7^5 \wedge \sum_{i=1}^{5} i x_i = 0 \ (\mod 7)\right\}$.

3 Exercise 3.

There is a cryptographic conference in Monaco. The best student of a cryptographic course will be allowed to participate. Keiko and Hiroki are students with the maximum number of points from exercises. Unfortunately, only one of them is allowed to participate so they have to decide which one. Hiroki is now abroad, therefore Keiko suggest the following protocol that allows them to remotely flip a coin.

- Keiko chooses either $x =$ "$HEAD$" or $x =$ "$TAIL$" and picks a random number k. She encrypts x with DES cipher using the key k. She obtains $y = DES_k(x)$.
- Keiko sends y to Hiroki.
- Hiroki flips a coin and tells Keiko which face is up.
- Keiko reveals k.
- Hiroki decrypts y with DES using the key k and obtains the guess of Keiko. If Keiko's guess is correct, she travels to Monte Carlo.

Is Keiko able to cheat?