Homework Assignment 1

Due date: October 11, 2018

It is possible to collect up to 110 points in this homework assignment.

Problem 1. Let $n = 2t$ for some $t \in \mathbb{N}$. Assume that the following $(n, 2, n)$ code

$$\mathcal{C} = \{\underbrace{00\cdots0}_{t \text{ zeroes}}\underbrace{11\cdots1}_{t \text{ ones}}, \underbrace{11\cdots1}_{t \text{ ones}}\underbrace{00\cdots0}_{t \text{ zeroes}}\}$$

is used to transmit one bit of information. Denote $\mathbb{F}_2 = \{0, 1\}$ and assume that the decoder $\mathcal{D} : \mathbb{F}_2^n \to \mathcal{C}$ is *maximum-likelihood.*

Codeword $\boldsymbol{c} = \underbrace{00\cdots0}_{t \text{ zeroes}}\underbrace{11\cdots1}_{t \text{ ones}}$ is transmitted through the BSC(p), $0 \le p < 1/2$.

(a) What is the probability that there are *exactly* s errors in $\boldsymbol{c}$, if $0 \le s \le n$?

(b) What is the probability that there are *at least* s errors in $\boldsymbol{c}$, $0 \le s \le n$?

(c) What is the probability P_n that $\mathcal{D}$ will make a decoding error?

(d) How P_n behaves when n grows? (You can assume that p is a very small positive number.)

Problem 2. In the multiplicative group $\mathbb{F}^*$ of a field $\mathbb{F}$, a *generator* is an element $g \in \mathbb{F}^*$ with a maximum possible multiplicative order, $\mathrm{o}(g) = |\mathbb{F}^*| = |\mathbb{F}| - 1$. In other words, powers of g generate all the elements of $\mathbb{F}^*$.

Find all generators in the multiplicative group of $\mathbb{F}_{11}$.

Problem 3. Let $\mathbb{F}$ be a finite field. In this question, we will show that for every $a \in \mathbb{F}$ it holds that $a^{|\mathbb{F}|} = a$. Recall that for each $a \in \mathbb{F}^*$, there exists an integer r, $1 \le r \le |\mathbb{F}^*|$, such that $a^r = 1$ (this r can vary for different a).

(a) Fix $a \in \mathbb{F}^*$. Consider the set of elements (for $r = \mathrm{o}(a)$, i.e. the smallest r for a)

$$H = \{1, a, a^2, a^3, \cdots, a^{r-1}\} .$$

Take an arbitrary $y \in \mathbb{F}^*$. Denote

$$H_y \triangleq \{y, ya, ya^2, ya^3, \cdots, ya^{r-1}\} .$$

Prove that for any $y_1, y_2 \in \mathbb{F}^*$ either (i) $H_{y_1} = H_{y_2}$ or (ii) H_{y_1} and H_{y_2} are mutually disjoint.

(b) Show that for any $y \in \mathbb{F}^*$ it holds $|H_y| = r$.

(c) Show that $|H|$ divides $|\mathbb{F}^*|$.

(d) Conclude that $a^{|\mathbb{F}|} = a$.

Problem 4. Let s and t be positive integers. Show that over *every* field, the polynomial $x^s - 1$ divides $x^t - 1$ if and only if $s \mid t$.