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
\[
C = \{ \overbrace{00\cdots0}^t \text{ zeroes}, \overbrace{11\cdots1}^t \text{ ones} \}
\]
is used to transmit one bit of information. Denote \( \mathbb{F}_2 = \{0,1\} \) and assume that the decoder \( D : \mathbb{F}_2^n \to C \) is maximum-likelihood.

Codeword \( c = \overbrace{00\cdots0}^t \text{ zeroes} \overbrace{11\cdots1}^t \text{ ones} \) is transmitted through the BSC\((p)\), \( 0 \leq p < 1/2 \).

(a) What is the probability that there are exactly \( s \) errors in \( c \), if \( 0 \leq s \leq n \)?
(b) What is the probability that there are at least \( s \) errors in \( c \), \( 0 \leq s \leq n \)?
(c) What is the probability \( P_n \) that \( D \) 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 \( \mathbb{F}^\ast \) of a field \( \mathbb{F} \), a generator is an element \( g \in \mathbb{F}^\ast \) with a maximum possible multiplicative order, \( o(g) = |\mathbb{F}^\ast| = |\mathbb{F}| - 1 \). In other words, powers of \( g \) generate all the elements of \( \mathbb{F}^\ast \).

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 \( a \in \mathbb{F}^\ast \), there exists an integer \( r, 1 \leq r \leq |\mathbb{F}|^\ast \), such that \( a^r = 1 \) (this \( r \) can vary for different \( a \)).

(a) Fix \( a \in \mathbb{F}^\ast \). Consider the set of elements (for \( r = o(a) \), i.e. the smallest \( r \) for \( a \))
\[
H = \{1, a, a^2, a^3, \ldots, a^{r-1} \}.
\]
Take an arbitrary \( y \in \mathbb{F}^\ast \). Denote
\[
H_y \triangleq \{ y, ya, ya^2, ya^3, \ldots, ya^{r-1} \}.
\]
Prove that for any \( y_1, y_2 \in \mathbb{F}^\ast \) 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 \( y \in \mathbb{F}^\ast \) it holds \( |H_y| = r \).
(c) Show that \( |H| \) divides \( |\mathbb{F}^\ast| \).
(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 $s \mid t$. 