Homework assignment 1

Due date: October 16, 2017

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

1. Let $n = 2t + 1$ for some $t \in \mathbb{N}$. Assume that the following binary $(n, 2, n)$ code
   \[ C = \{(1, 0, 1, 0, \cdots, 1, 0, 1), (0, 1, 0, 1, \cdots, 0, 1, 0)\} \]

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

   Codeword $\bar{c} = (1, 0, 1, 0, \cdots, 1, 0, 1)$ is transmitted through the BSC($p$), $0 \leq p < \frac{1}{2}$.

   (a) What is the probability that there are exactly $s$ errors in $\bar{c}$, if $0 \leq s \leq n$?
   (b) What is the probability that there are at least $s$ errors in $\bar{c}$, $0 \leq s \leq n$?
   (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 very small.)

2. (a) Find multiplicative orders of all elements in $\mathbb{F}_{11}$.
   (b) Demonstrate that all multiplicative orders in (a) divide the order (size) of the multiplicative group $F^*$ of $\mathbb{F}_{11}$.

3. Let $\mathbb{F} = (F, +, \cdot)$ be a finite field. In this question, we will show that for every $a \in F$ it holds that $a^{\vert F \vert} = a$ (here $\vert F \vert$ denotes the size of $F$). Recall that for each $a \in F$, $a \neq 0$, there exists an integer $r$, $1 \leq r \leq \vert F \vert - 1$, such that $a^r = 1$ (this $r$ can vary for different $a$).

   (a) Fix $a \in F^*$. Consider the set of elements (for the smallest possible $r$ from the part (a))
      \[ H = \{1, a, a^2, a^3, \cdots, a^{r-1}\} \]

      Take an arbitrary $y \in F$, $y \neq 0$. Denote
      \[ H_y = \{y, ya^2, ya^3, \cdots, ya^{r-1}\} \]

      Prove that for any $y_1, y_2 \in F^*$ 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 $y \in F^*$ it holds $\vert H_y \vert = r$.
   (c) Show that $\vert H \vert$ divides $\vert F \vert - 1$.
   (d) Conclude that $a^{\vert F \vert} = a$.

4. Let $F = \{0, 1\}$, and let $\bar{x}$, $\bar{y}$ and $\bar{z}$ be words in $F^n$ such that
   \[ d(\bar{x}, \bar{y}) = d(\bar{y}, \bar{z}) = d(\bar{z}, \bar{x}) = 2t \]
   for some $t \geq 1$, $t \in \mathbb{N}$. Show that there exists exactly one word $\bar{v}$ in $F^n$ such that
   \[ d(\bar{x}, \bar{v}) = d(\bar{y}, \bar{v}) = d(\bar{z}, \bar{v}) = t \].