MTAT.05.082: Introduction to Coding Theory **University of Tartu**

Homework Assignment 1

Due date: October 11, 2018
Solution

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 $0 \le s \le n$?

Solution. These s errors can happen on any s positions out of n positions of the transmitted codeword. When the positions of the errors are fixed, to find a probability of the event "errors happened on exactly these s positions", we need to multiply the probabilities of errors happening, p, on these positions and not happening, $1 - p$, on the rest $n - s$ positions, i.e.

$$\binom{n}{s} p^s (1-p)^{n-s}. \qquad \blacksquare$$

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

Solution. At least s errors effectively means that there are s errors, or $s + 1$ errors, or $s + 2$ errors, ..., or n errors. So the answer is just a sum:

$$\sum_{i=s}^{n} \binom{n}{i} p^i (1-p)^{n-i}. \qquad \blacksquare$$

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

Solution. The decoder makes an error if and only if there were more than or equal to half of errors, i.e. more than or equal to $n/2 = t$. Hence, $\mathcal{D}$ makes a decoding error if and only if there were *at least* t errors. Using the previous result with $s = t$, we obtain:

$$P_n = \sum_{i=t}^{n} \binom{n}{i} p^i (1-p)^{n-i} = \sum_{i=t}^{2t} \binom{2t}{i} p^i (1-p)^{2t-i}. \qquad \blacksquare$$

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

Solution. We need to find $\lim\limits_{n\to\infty} P_n = \lim\limits_{t\to\infty} P_n$. For that we bound P_n from above:

$$P_n = \sum_{i=t}^{2t} \binom{2t}{i} p^i (1-p)^{2t-i} < \sum_{i=t}^{2t} \binom{2t}{i} p^t \cdot 1$$

$$= p^t \sum_{i=t}^{2t} \binom{2t}{i} < p^t \sum_{i=0}^{2t} \binom{2t}{i} = p^t 2^{2t} = (4p)^t \xrightarrow[t\to\infty]{} 0\,,$$

provided $4p < 1$ (which is true if $p < 1/4$).

Note: it can be proven that $P_n \to 0$ even for larger p (but still $p < 1/2$); however we suggest the aforementioned proof for the sake of simplicity. ■

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 $\mathbb{F}_{11}$.

Solution. Let put powers of elements of $\mathbb{F}_{11}$ in a Table 1.

Table 1: Powers of non-zero elements of $\mathbb{F}_{11}$

α	degree:									
	1	2	3	4	5	6	7	8	9	10
1	1									
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1					
4	4	5	9	3	1					
5	5	3	4	9	1					
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1					
10	10	1								

Therefore, the elements 2, 6, 7, and 8 are generators 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.

Solution. Take arbitrary $y_1 \neq y_2 \in F^*$. If $H_{y_1} \cap H_{y_2} = \varnothing$, we are fine.

Now assume these two sets have a common element, i.e. there exist i and j such that $y_1 a^i = y_2 a^j$ (note that $y_1 a^i \in H_{y_1}$ and $y_2 a^j \in H_{y_2}$). Then $y_2 = y_1 a^{i-j}$ and for each integer k we have $y_2 a^k = y_1 a^{i-j+k} \in H_{y_1}$, i.e. each element of H_{y_2} is also an element of H_{y_1}. Analogously, $y_1 = y_2 a^{j-i}$ and for each integer ℓ we have $y_1 a^\ell = y_2 a^{j-i+\ell}$, i.e. each element of H_{y_1} is also an element of H_{y_2}.

Hence we assumed that H_{y_1} and H_{y_2} have one common element and from that we proved that the sets are equal. This proves the statement of the problem. ■

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

Solution. We defined H_y as a list of r elements. So the two possibilities are:

(i) all r elements being different (and then $|H_y| = r$), or
(ii) some elements repeat (and then $|H_y| < r$).

We would like to show that the latter is not possible for any $y \in F^*$.

Assume to the contrary that there are two equal elements, say $ya^i = ya^j$ for some $0 \leq i < j \leq r-1$. Then consider element a^{j-i}. From $ya^i = ya^j$ we obtain that $a^i = a^j$ and hence $1 = a^{j-i}$.

We are previously given that r is the *minimum* positive integer such that $a^r = 1$. On the other hand, we have just built $r' = j - i < r$ with $a^{r'} = 1$. This contradiction proves that such i and j does not exist and all the elements of H_y are indeed different. ■

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

Solution. From (a) we know that each element $x \in F^*$ belongs to one and only one H_y (for some y), i.e. the set F^* splits without overlapping into ℓ subsets $H_{y_1}, H_{y_2}, \ldots, H_{y_\ell}$, each of them having size r (see (b)). Then the total size $|F^*| = |H_{y_1}| + |H_{y_2}| + \cdots + |H_{y_\ell}| = r\ell$, which is obviously divisible by r. But $|F^*| = |F| - 1$. Therefore we proved the statement of the problem. ■

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

Solution. As we have just shown, $|F| - 1$ is divisible by r, precisely, $|F| - 1 = r\ell$.

Then

$$a^{|F|} = a^{r\ell+1} = a \cdot (a^r)^\ell = a \cdot 1^\ell = a .$$

■

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 $s \mid t$.

Solution.

$\Leftarrow$) Assume that $s \mid t$. Hence, we can represent $t = ds$. If we denote $y \triangleq x^s$, we can write

$$\begin{aligned} x^t - 1 &= y^d - 1 \\ &= (y-1)(y^{d-1} + y^{d-2} + \cdots + y + 1) \\ &= (x^s - 1)(x^{s(d-1)} + x^{s(d-2)} + \cdots + x^s + 1) \\ &= 0 \pmod{(x^s - 1)}. \end{aligned}$$

$\Rightarrow$) Assume that

$$x^t - 1 = 0 \pmod{(x^s - 1)} \tag{1}$$

and divide t by s with a remainder: $t = ds + r$, $r < s$.

We write:

$$\begin{aligned} x^t - 1 &= x^{ds+r} - x^r + x^r - 1 \\ &= x^r(x^{ds} - 1) + x^r - 1 \\ &= x^r(x^s - 1)(x^{s(d-1)} + x^{s(d-2)} + \cdots + x^s + 1) + x^r - 1 \\ &= x^r - 1 \pmod{(x^s - 1)}. \end{aligned} \tag{2}$$

Comparing (1) and (2), we get:

$$x^r - 1 = 0 \pmod{(x^s - 1)}.$$

Therefore, for some polynomial $p(x)$, it holds that

$$x^r - 1 = p(x)(x^s - 1).$$

If $p(x)$ is non-zero (and, therefore, $x^r - 1$ is non-zero), it has a non-negative degree $n \geq 0$. Then we should have the following for degrees of polynomials:

$$r = n + s \geq s,$$

which is not possible (recall $r < s$). Therefore the only possibility is that $p(x)$ is the zero polynomial and, hence, $x^r - 1$ is the zero polynomial too. The latter means that $r = 0$. Hence, $t = ds + r = ds$ and $s|t$.

■