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

Homework Assignment 5

Due date: December 13, 2018

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

1. Consider Shamir's secret sharing scheme over $\mathbb{F}_5$ with $n = 4$ and $k = 3$. Let $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 3$ and $\alpha_4 = 4$. Assume that the secret s is selected randomly and uniformly in $\mathbb{F}_5$. User 1 knows that $P(\alpha_1) = 1$, user 2 knows that $P(\alpha_2) = 0$, user 3 knows that $P(\alpha_3) = 3$, and user 4 knows that $P(\alpha_4) = 0$, where $P(x) = a_2x^2 + a_1x + s$.

   (a) Show that if users 2 and 3 try to find s, then any value of $s \in \mathbb{F}_5$ is equally probable.

   (b) Show that users 2, 3 and 4 jointly can find s. What is the value of s?

2. Let $a(x)$ and $b(x)$ be two nonzero polynomials over a finite field $\mathbb{F}$ such that $\deg(a(x)) > \deg(b(x))$. Consider the extended Euclid's algorithm, which was presented in the lecture (for your convenience that algorithm also appears in the appendix at the end of this homework). Let τ be the largest index i such that $r_i(x) \neq 0$. Show by induction on i:

   (a) For all $i = 0, 1, 2, \cdots, \tau$ we have $s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x) = (-1)^{i+1}$.

   (b) For all $i = -1, 0, 1, \cdots, \tau + 1$ we have $s_i(x)a(x) + t_i(x)b(x) = r_i(x)$.

   (c) For all $i = 1, 2, \cdots, \tau + 1$ we have $\deg(t_i(x)) + \deg(r_{i-1}(x)) = \deg(a(x))$. (Hint: you can use (a) and (b).)

3. For a polynomial $a(x) = \sum_{i=0}^{n} a_i x^i$ over a finite field $\mathbb{F}$ define a formal derivative of $a(x)$ to be

$$a'(x) = \sum_{i=1}^{n} i \cdot a_i x^{i-1} \ .$$

   Let $a(x)$ and $b(x)$ be two polynomials (of possibly different degrees) over $\mathbb{F}$, and $c \in \mathbb{F}$. Show that:

   (a) $(a(x) + b(x))' = a'(x) + b'(x)$.

   (b) $(c \cdot a(x))' = c \cdot a'(x)$.

   (c) $(a(x) \cdot b(x))' = a(x) \cdot b'(x) + a'(x) \cdot b(x)$.

4. Let $\mathbb{F} = \mathbb{F}_7$. Suppose that $\mathcal{C}$ is a $[6, 2, 5]$ Reed-Solomon code over $\mathbb{F}$, with a parity-check matrix given by

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 \end{pmatrix} .$$

Assume that $\bar{\mathbf{c}} \in (\mathbb{F})^6$ is transmitted, and $\bar{\mathbf{y}} = (5, 1, 1, 6, 4, 4) \in (\mathbb{F})^6$ is received. In this question, you will show steps of the decoding of $\bar{\mathbf{y}}$ by using Euclid's algorithm. Please show all the steps in the algorithm you apply.

(a) Find the syndrome polynomial $S(x)$.

(b) Show execution of the extended Euclid's algorithm applied to $a(x) = x^{d-1}$ and to $S(x)$.

(c) Find the error-locator and the error-evaluator polynomials.

(d) What are the locations and the values of the errors?

(e) What is $\mathbf{c}$ if we assume that there were at most $\lfloor (d-1)/2 \rfloor$ errors?

Appendix

$r_{-1}(x) = a(x); \quad r_0(x) = b(x);$
$s_{-1}(x) = 1; \qquad s_0(x) = 0;$
$t_{-1}(x) = 0; \qquad t_0(x) = 1;$
for $(\ i = 1;\ r_{i-1}(x) \neq 0;\ i{+}{+}\ )\ \{$
$\quad r_{i-2}(x) = \underline{q_i(x)} \cdot r_{i-1}(x) + \underline{r_i(x)};$
$\quad s_{i-2}(x) = q_i(x) \cdot s_{i-1}(x) + \underline{s_i(x)};$
$\quad t_{i-2}(x) = q_i(x) \cdot t_{i-1}(x) + \underline{t_i(x)};$
$\}$

Extended Euclid's algorithm.