Homework Assignment 5

Due date: December 5, 2016

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

1. Let \( C \) be an \([n, k, 3]\) Reed-Solomon code, and \( H \) its parity-check matrix with code locators \( \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F} \) and column multipliers \( v_1 = v_2 = \cdots = v_n = 1 \).

   (a) A codeword of \( C \) is transmitted through a channel with errors, and a word \( y \in \mathbb{F}^n \) is received with one error at location \( j \). Let \( (s_0, s_1)^T \) be the syndrome of \( y \) with respect to \( H \). Show that
   \[ \alpha_j = \frac{s_1}{s_0}, \]
   and that the error value is equal to \( s_0 \).

   (b) A codeword \( c = (c_1, c_2, \ldots, c_n) \in C \) is transmitted through an erasure channel, and a word \( y = (y_1, y_2, \ldots, y_n) \in (\mathbb{F} \cup \{\text{?}\})^n \) is received, where ‘?’ denotes an erasure. The word \( y \) contains two erasures, whose locations are denoted by \( i \) and \( j \).
   The syndrome of \( y \) is computed as in the first part where, for the purpose of this computation, 0 is substituted for \( y_i \) and \( y_j \). Show that the entries of \( c \) at the erased locations are given by
   \[ c_i = \frac{s_1 - \alpha_j s_0}{\alpha_j - \alpha_i} \quad \text{and} \quad c_j = \frac{s_1 - \alpha_i s_0}{\alpha_i - \alpha_j}. \]

2. Alice communicates with Bob by using coset coding over \( \mathbb{F}_7 \). She wants to send a message \((s_1, s_2, s_3)\) securely. In order to do so, Alice picks a random solution \( \bar{x} = (x_1, x_2, x_3, x_4, x_5) \) of the system
   \[ H \cdot \bar{x}^T = (s_1, s_2, s_3)^T, \]
   and sends it to Bob, where \( H \) is the following matrix
   \[ H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 2^2 & 3^2 & 4^2 & 5^2 \end{pmatrix}. \]

   (a) What are the parameters \( n, k \) and \( d \) of the code defined by \( H \), when used as a parity-check matrix? Prove.

   (b) How many different solutions \((x_1, x_2, x_3, x_4, x_5)\) can Alice choose from?

   (c) Assume that wiretapper Eve intercepts \( x_2 = 2 \) and \( x_5 = 5 \). Show that Eve does not know anything about the syndrome \((s_1, s_2, s_3)\) that was sent. In other words, show that from Eve’s point of view, any syndrome \((s_1, s_2, s_3)\) is possible.

   (d) Assume now that Eve intercepts \( x_1 = 1 \), in addition to \( x_2 = 2 \) and \( x_5 = 5 \). Show that now Eve has some knowledge about the syndrome \((s_1, s_2, s_3)\). Is this knowledge sufficient to determine \((s_1, s_2, s_3)\) in a unique way?
(e) Assume now that Eve intercepts $x_3 = 0$, in addition to $x_1 = 1$, $x_2 = 2$ and $x_5 = 5$. Is this knowledge sufficient to determine $(s_1, s_2, s_3)$ in a unique way?

3. Consider Shamir’s secret sharing scheme over $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ with $n = 4$ and $k = 4$. 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 $\mathbb{F}_5$. The user 1 knows that $P(\alpha_1) = 0$, the user 2 knows that $P(\alpha_2) = 1$, the user 3 knows that $P(\alpha_3) = 2$, and the user 4 knows that $P(\alpha_4) = 0$, where $P(x) = a_3 x^3 + a_2 x^2 + a_1 x + s$.

(a) Show that if the users 1, 2 and 3 try to find $s$, then any value of $s \in \mathbb{F}_5$ is equally probable.

(b) Show that the users 1, 2, 3 and 4 jointly can find $s$. What is the value of $s$?

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

2