Homework Assignment 1

Due on March 31, 2011

In the following $\mathbb{F}_q$ denotes a finite field of q elements.

1. Let $\mathbb{F}_{q^n}$ be a degree n extension of the finite field $\mathbb{F}_q$. Show that the trace and the norm maps $\mathbb{F}_{q^n} \to \mathbb{F}_q$ are surjective.
2. Let β be a primitive element of $\mathbb{F}_{64}$ and $m_i(x)$ the minimal polynomial of β^i over $\mathbb{F}_2$. Let C be the cyclic code (over $\mathbb{F}_2$) generated by $g(x) = m_1(x) \cdot m_3(x) \cdot m_5(x)$ in $\mathbb{F}_2[x]/(x^{63} - 1)$. Find the dimension and the distance of the code C.
3. Let $C = (g(x)) \subset \mathbb{F}_q[x]/(x^n - 1)$ be the cyclic code of length n over $\mathbb{F}_q$ generated by $g(x)$ where $g(x)$ is a factor of $x^n - 1$ over $\mathbb{F}_q$. Write $x^n - 1 = g(x)h(x)$ and $h(x) = \sum_{i=0}^{k} h_i x^i$. Show that the parity checking matrix can be taken to be the $(n-k) \times n$ matrix
$$H = \begin{pmatrix} 0 & \cdots & & 0 & h_k & \cdots & h_1 & h_0 \\ 0 & \cdots & & h_k & h_{k-1} & \cdots & h_0 & 0 \\ & \ddots & & & & \ddots & & \\ h_k & \cdots & h_0 & 0 & & \cdots & & 0 \end{pmatrix}.$$
4. Determine the numbers of irreducible monic polynomials of degree 2, 3, 4, 5, and 6 over $\mathbb{F}_q$.
5. Show that
$$\sum_{\beta \in \mathbb{F}_q} \beta^n = \begin{cases} -1 & \text{if } (q-1) \mid n \\ 0 & \text{if } (q-1) \nmid n. \end{cases}$$
6. Describe the dual code of a generalized Reed-Solomon code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ over $\mathbb{F}_q$ in terms of the evaluations of certain polynomials.