COMPUTATIONAL ALGEBRA 17/09/14

1. Let $\mathcal{C}$ be the linear code over $\mathbb{F}_2$ with parity check matrix H

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

   (a) Find the length, the dimension, and the minimum distance of $\mathcal{C}$.

   (b) Find all the elements of $\mathcal{C}$.

   (c) Find a generator matrix G of $\mathcal{C}$.

   (d) Encode the vector $(101) \in \mathbb{F}_2^3$ using the matrix H and the matrix G

   (e) Find the vectors in $\mathbb{F}_2^3$ corresponding to (110011).

2. (a) Find a primitive element of $\mathbb{F}_{11}$.

   (b) Construct a Reed-Solomon code $\mathcal{C}$ of dimensions $[10, 5]$ over $\mathbb{F}_{11}$.

   (c) Determine the minimal distance of $\mathcal{C}$.

   (d) Find a parity check matrix for $\mathcal{C}$.

3. (a) Show that the polynomial $f(x) = x^3 + x + 1 \in \mathbb{F}_2$ is irreducible over $\mathbb{F}_2$

   (b) Construct the field $\mathbb{F}_8$ using the polynomial $f(x)$;

   (c) Let α be a root of $f(x)$. Construct a table with each vector in $\mathbb{F}^3$ associated to the powers of α and to 0.

   (d) Which powers of α are primitive elements of $\mathbb{F}_8$?

4. Determine the splitting field of

   (a) $x^5 + x^4 + 1$ over $\mathbb{F}_2$

   (b) $x^3 + x^2$ over $\mathbb{F}_3$. Does it split in $\mathbb{F}_{27}$?

5. Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$.

   (a) Give the definition of the generator polynomial of $\mathcal{C}$

   (b) Show that if $g(x)$ is the generator polynomial of $\mathcal{C}$ and $k = n - \deg g(x)$, then $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ is a basis for $\mathcal{C}$.

6. (a) Let K the smallest field of characteristic 2 containing a primitive 15-th root of unity. Determine the number of elements of K and find a primitive element of K.

   (b) Let α be a primitive element of $\mathbb{F}_{2^n}$. Determine the degree of the minimal polynomial f_α over $\mathbb{F}_2$. Which is its splitting field?