COMPUTATIONAL ALGEBRA 24/06/14

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

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

   (a) Find the parity check of $\mathcal{C}$

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

   (c) Using the code $\mathcal{C}$, encode the vector $(110) \in \mathbb{F}_2^3$

   (d) Using the Syndrome Decoding Algorithm, correct the received vectors $y_1 = (101001)$ and $y_2 = (101110)$. Denoted by c_1 and c_2 the corrected vectors, verify that c_1 and c_2 are codewords.

   (e) Decode c_1 and c_2 (i.e find the vectors in $\mathbb{F}_2^3$ corresponding to c_1 and c_2).

2. (a) Find the lattice of subfields of $\mathbb{F}_{64}$.

   (b) The field $\mathbb{F}_{27}$ is contained in the field $\mathbb{F}_{81}$?

   (c) The polynomial $x^5 - 1 \in \mathbb{F}_2[x]$ splits in $\mathbb{F}_{32}[x]$? And in $\mathbb{F}_{256}[x]$?

3. (a) Construct the field $\mathbb{F}_8$;

   (b) find the primitive elements of $\mathbb{F}_8$

   (c) Is is true that a primitive 7^{th}-root of the unit over $\mathbb{F}_2$ belongs to $\mathbb{F}_8$? Why? If yes, find such a root α.

4. Let $\mathcal{C}$ the cyclic code of length 7 over $\mathbb{F}_2$ with idempotent polynomial $e(x) = 1 + x^3 + x^5 + x^6$

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

   (b) Apply the BCH bound to study the minimum distance of $\mathcal{C}$.

5. Give the definition of a cyclic code of length n over $\mathbb{F}_q$. Show that the cyclic codes of length n over $\mathbb{F}_q$ correspond to the ideals of the ring $\mathbb{F}_q[x]/(x^n - 1)$.