Homework Assignment 3

Due date: November 19, 2018

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

1. Show that in every linear code $\mathcal{C}$ over $\mathbb{F}_2$, either all codewords have even Hamming weight or exactly half of the codewords have even Hamming weight.

   Hints:

   - Observe that the sum of two even-weight words over $\mathbb{F}_2$ has even weight, the sum of two odd-weight words has even weight, and the sum of an even-weight word and an odd-weight word has odd weight.
   - Take some odd-weight word $\bar{\boldsymbol{c}} \in \mathcal{C}$ and consider all words $\bar{\boldsymbol{c}} + \bar{\boldsymbol{x}}$, where $\bar{\boldsymbol{x}}$ varies over all even-weight words in $\mathcal{C}$.

2. Let $\mathbb{F} = \mathbb{F}_{2^4}$ be a field represented as a residue ring of the polynomials over $\mathbb{F}_2$ modulo the polynomial $\beta^4 + \beta^3 + \beta^2 + \beta + 1$.

   (a) Express each element in $\mathbb{F}$ as a power of a primitive element $\beta + 1$ (present the results in the table similarly to the table that was shown in the class).[1]

   (b) Compute in this field: $\beta^2 + \beta^4$, $\beta^2(\beta + 1)^3$, $(\beta^2 + 1)^{-1}$.

3. Let Φ be an extension field of $\mathbb{F}_3$ of extension degree $s > 1$. Let $a(x)$ be a nonzero polynomial with the coefficients in $\mathbb{F}_3$.

   (a) Show that if β is a root of the polynomial $a(x)$ over Φ, then $\{\beta^3, \beta^{3^2}, \beta^{3^3}, \beta^{3^4}, \cdots\}$ are all roots of $a(x)$ over Φ.

   (b) Show that if β is a primitive element in Φ, and β is a root of $a(x)$, then the degree of $a(x)$ is at least s.

4. Let $\mathcal{C}_1$ be a linear $[n, k_1, d_1]$ code and $\mathcal{C}_2$ be a linear $[n, k_2, d_2]$ code over the same field $\mathbb{F}$. Define the code

   $$\mathcal{C}_3 = \{ \ (\ \bar{\boldsymbol{c}}_1 \mid \bar{\boldsymbol{c}}_1 + \bar{\boldsymbol{c}}_2 \ ) \ : \ \bar{\boldsymbol{c}}_1 \in \mathcal{C}_1 \text{ and } \bar{\boldsymbol{c}}_2 \in \mathcal{C}_2 \} \ .$$

   Show that $\mathcal{C}_3$ is a linear $[2n, k, d]$ code over $\mathbb{F}$, where $k = k_1 + k_2$ and $d = \min\{2d_1, d_2\}$.

---

[1] Note that β is not a primitive element in this field.