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 $C$ over $F_2$, 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 $F_2$ 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 $\bar{c} \in C$ and consider all words $\bar{c} + \bar{x}$, where $\bar{x}$ varies over all even-weight words in $C$.

2. Let $F = F_{2^4}$ be a field represented as a residue ring of the polynomials over $F_2$ modulo the polynomial $\beta^4 + \beta^3 + \beta^2 + \beta + 1$.

   (a) Express each element in $F$ 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 $\Phi$ be an extension field of $F_3$ of extension degree $s > 1$. Let $a(x)$ be a nonzero polynomial with the coefficients in $F_3$.

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

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

4. Let $C_1$ be a linear $[n, k_1, d_1]$ code and $C_2$ be a linear $[n, k_2, d_2]$ code over the same field $F$.

   Define the code
   
   $$C_3 = \{ (\bar{c}_1 | \bar{c}_2) : \bar{c}_1 \in C_1 \text{ and } \bar{c}_2 \in C_2 \} .$$

   Show that $C_3$ is a linear $[2n, k, d]$ code over $F$, where $k = k_1 + k_2$ and $d = \min\{2d_1, d_2\}$.

---

\(^1\)Note that $\beta$ is not a primitive element in this field.