Exercise Sheet 6

Exercise 6.1. Count the number of linear cyclic codes of length 8 over $\mathbb{F}_3$.

Exercise 6.2. In this exercise, we design a 2-error-correcting BCH code of length 13, and dimension 6 over $\mathbb{F}_3$.

1. If ω denotes a primitive 13th root of unity over $\mathbb{F}_3$, show that the smallest extension field of $\mathbb{F}_3$ in which ω lives has degree 3.
2. Let $g_i(x)$ denote the minimal polynomial of ω^i over $\mathbb{F}_3$. What is a generator polynomial of a 2-error correcting BCH code of length 13 and dimension 6 in terms of the $g_i(x)$?
3. Now we want to calculate the polynomials $g_i(x)$. First, find an irreducible polynomial of degree 3 over $\mathbb{F}_3$.
4. Use the irreducible polynomial obtained in the previous part to find a primitive element α in a degree 3 extension of $\mathbb{F}_3$, and show that we can choose $\omega := \alpha^2$. Calculate the minimal polynomials $g_0(x), g_1(x), g_2(x), g_4(x), g_7(x)$, and show that this is the complete list of $g_i(x)$.
5. Now compute the generator polynomial for the code.
6. Suppose that we have received the word $y := (0, -1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$. Apply the decoding algorithm that we saw in the lecture to decode this string to its nearest codeword.