Exercise Sheet 7

Exercise 7.1. Show that the binary BCH code of length $n = 2^m - 1$ with assigned distance 1 is a Hamming code.

Exercise 7.2. Let $\mathbb{F}_9$ be defined as $\mathbb{F}_3[\omega]$ where $\omega^2 = -1$ and define $\beta = 1 + \omega$. A BCH code of designed distance 4 and associated with the first powers of β (β^0, β^1, ...) is being used. We receive $y(z) = 1 + z + z^7$.

1. Construct the power table of β.

2. Find the generating polynomial $g(x)$ of the code. What are the parameters of the code? How many errors can this code accept ?

3. Decode the received message.

Exercise 7.3.

1. Design a 3 error-correcting BCH code of length 31 and dimension 16 over $\mathbb{F}_2$.

2. Suppose that $S_i = X^i + Y^i + Z^i$ (for $i = 1, \ldots, 6$) are the syndromes for a received word. Write expressions for $\sigma_2 = XY + YZ + XZ$ and $\sigma_3 = XYZ$ as rational functions in $S_1, \ldots, S_6$.

3. Design a decoding algorithm for the code.