Final
Algebraic Coding Theory
Math 525
Stephen Giang RedID: 823184070

Problem 1:

(a) Find a parity-check matrix H for a cyclic Hamming code of length 15 using GF(2^4)constructed from $1+x+x^4$(see Table 5.1, p. 114), where the generator polynomial is $m_7(x)$. Each entry of H must be expressed as a power of β, where β is the primitive element of the field, exactly as in Table 5.1.

Notice the generator polynomial: $m_7(x)$

$$[\beta^7] \Rightarrow [\beta^{14}] \Rightarrow [\beta^{28} = \beta^{13}] \Rightarrow [\beta^{26} = \beta^{11}] \Rightarrow [\beta^{22} = \beta^7]$$

$$\begin{aligned}
m_7(x) &= (x+\beta^7)(x+\beta^{14})(x+\beta^{13})(x+\beta^{11}) \\
&= \left(x^2 + (\beta^7+\beta^{14})x + \beta^{21}\right)\left(x^2 + (\beta^{13}+\beta^{11})x + \beta^{24}\right) \\
&= \left(x^2 + \beta x + \beta^6\right)\left(x^2 + \beta^4 x + \beta^9\right) \\
&= x^4 + \left(\beta + \beta^4\right)x^3 + \left(\beta^9 + \beta^5 + \beta^6\right)x^2 + \left(\beta^{10} + \beta^{10}\right)x + \beta^{15} \\
&= x^4 + x^3 + 1
\end{aligned}$$

We get the Parity Check Matrix below:

$$H = \begin{bmatrix} 1 \\ \beta^7 \\ \beta^{14} \end{bmatrix}$$

(b) Now suppose r is received, where r is the word of length 15 that you obtained from your last name. Find the most likely codeword transmitted.

Notice my last name is GIANG, so we get

$$r(x) = \{00100\,10010\,01010\}(ANG) = x^2 + x^5 + x^8 + x^{11} + x^{13}$$

Notice the following:

$$r(\beta) = \beta^2 + \beta^5 + \beta^8 + \beta^{11} + \beta^{13} = \beta^2$$

Thus we get the most likely codeword is $\{01100\,10010\,01010\}$ (ING).