Mike O'Sullivan
Department of Mathematics
San Diego State University

Spring 2006

Math 625: Coding Theory

Homework III

Problem 1: In the section called Key Polynomials, we use the matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \dots & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \dots & \alpha^{-k-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \dots & \alpha^{-2k-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \dots & \alpha^{-3k-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{n-1} & \alpha^{n-2} & \dots & \dots & \alpha^{k+1} \end{bmatrix}$$

as check matrix. Determine the generator polynomial for this code. Determine the generator polynomial for the dual code. Draw the circuit for non-systematic encoding using multiplication by the generator polynomial. Draw the circuit for systematic encoding.

Problem 2: Let $\alpha \in \mathbb{F}_{16}$ satisfy $\alpha^4 = \alpha + 1$. Draw circuitry for multiplication by α^7.

Problem 3: Let $f(x) = \sum_{i=0}^{m} f_i x^i$ be a polynomial of degree m and let α be a constant. Horner's method for the computation of $f(\alpha)$ is iterative

$$\begin{aligned} c_0 &= f_m \\ c_i &= f_{m-i} + c_{i-1} * \alpha \end{aligned}$$

Prove inductively that $c_k = \sum_{i=m-k}^{m} f_i \alpha^{i-m+k}$. Conclude that $c_m = f(\alpha)$. Show that Horner's method may be implemented by the circuit given in class.

Problem 4: Let e be an error vector and let $f^e(x)$ be the error locator and $\phi^e(x)$ the error evaluator polynomials as described in the notes. Prove that for each i such that $e_i \neq 0$,

$$e_i = \frac{\phi^e(\alpha^i)}{(f^e)'(\alpha^i)}$$

Problem 5: Let $\alpha \in \mathbb{F}_9$ satisfy $\alpha^2 = \alpha + 1$. We will use the code $RS(n-k)^{\perp}$ which has dimension 5. Use Magma or Maple to compute the generator polynomial. Systematically encode $x^2 + 1$ for this code (do this by hand).