# EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2011

Assignment 4 : **20 points** **Due date**: November 11, 2011

Each of the following exercises is worth 5 points. Every nontrivial step in a proof should be accompanied by justification.

1. Let $\mathbb{F}_{16}$ be the field generated by $p(X) = 1 + X + X^4$. Let $\alpha$ be a primitive element of $\mathbb{F}_{16}$ which is a root of $p(X)$. Devise a circuit which is capable of multiplying any element in $\mathbf{F}_{16}$ by $\alpha^7$.

2. Consider a $t$-error-correcting binary BCH code of length $n = 2^m - 1$. If $2t+1$ is a factor of $n$, prove that the minimum distance of the code is exactly$2t + 1$. You can assume the BCH bound in your solution ($d_{min} \geq 2t + 1$). (*Hint:* Let $n = l(2t + 1)$. Show that $\frac{X^n+1}{X^l+1}$ is a code polynomial of weight $2t + 1$. Remember that a code polynomial has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ as roots where $\alpha$ is a primitive element of $\mathbb{F}_{2^m}$ which has order $n = 2^m - 1$.)

3. Prove that the dual of a Reed-Solomon code is a Reed-Solomon code. (*Hint*: The dual code of an $(n, k)$ cyclic code with generator polynomial $g(X)$ has generator polynomial $X^k h(X^{-1})$ where $h(X) = \frac{X^n - 1}{g(X)}$.)

4. Consider a $(2, 1)$ convolutional code with encoder matrix $G(D) = \begin{bmatrix} 1 + D^2 & 1 + D + D^2 + D^3 \end{bmatrix}$.

   (a) Draw the encoder circuit.

   (b) Draw the encoder state diagram.

   (c) Is this encoder catastrophic? If yes, find an infinite weight information sequence which generates a codeword of finite weight.