ECE/MATH 641: HOMEWORK 3, DUE OCT 27.

Please solve the following problems.

1. Show that the polynomial $x^4 + x^3 + x^2 + x + 1$, with coefficients in $\mathbf{F}_2$, is irreducible. Using this polynomial, describe $\mathbf{F}_{16}$ as a set, including how addition and multiplication are defined.

2. Find an explicit element β of order 15 in the above $\mathbf{F}_{16}$, meaning that the smallest positive integer n such that $\beta^n = 1$ is 15. With a suitable choice of k, will the $[15, k]$ Reed-Solomon code produced using the powers of β ever have the same parameters as the Hamming or simplex code of that length?

3. Let C be a binary $[16, 8, 6]$ code with weight enumerator $A(x, y) = x^{16} + 112x^{10}y^6 + 30x^8y^8 + 112x^6y^{10} + y^{16}$. Suppose that C is used on a Binary Symmetric Channel with probability p of bit-flip.

(a) How many errors can C correct?

(b) What is the probability of decoding failure for $p = 0.005$ if the code is used to correct 2 errors?

4. Let C be a $[10, 6]$ Reed-Solomon code over $\mathbf{F}_{11}$.

(a) Prove that 2 is a primitive element of $\mathbf{F}_{11}$. Is it true that all of the elements $2, 3, 4, ..., 10$ are primitive?

(b) Using the powers of 2, write out a parity-check matrix H for C. How many codewords does C contain?

(c) Let $r = (3, 0, 0, 10, 5, 4, 0, 6, 10, 0)$ be a received vector. Decode the vector to codeword c and find f such that $c = \text{eval}(f)$.

Typeset by $\mathcal{AMS}$-TEX