ECE/MATH 641 PRACTICE MIDTERM

Nigel Boston

For full credit you must explain your reasoning. Each question is worth an equal amount. Answer them in any order.

1. Let $f(x) = x^5 + x^2 + 1$, where its coefficients are in $\mathbf{F}_2$. Let α be a zero of $f(x)$ in $\mathbf{F}_{32}$.

(a) Why must α be primitive?

(b) Show that α^3 is a zero of $m(x) = x^5 + x^4 + x^3 + x^2 + 1$.

(c) Define a BCH code C to be those polynomials $c(x)$ over $\mathbf{F}_2$ of degree < 32 such that $c(\alpha) = c(\alpha^3) = 0$. Find a generator polynomial for C and show that the minimum distance of C is 5.

(d) Assuming that a codeword $c(x)$ is transmitted and $r(x)$ received, such that $r(\alpha) = 1, r(\alpha^3) = \alpha^7 + 1$, where are the errors in $r(x)$?

2. (a) Let $g(x) = x^5 + x^4 + x^2 + 1$, where its coefficients are in $\mathbf{F}_2$. Let C be the binary cyclic code with generator polynomial $g(x)$. Find a parity check matrix for C.

(b) Find the minimum distance of C.

(c) Assume you have received a vector where either one digit is wrong or two neighbouring digits have changed place. How can you find the codeword that was sent?

(d) For which values of k is there a binary cyclic $[13, k, 3]$ code?

3. Consider an $[n, k]$ Reed-Solomon code where $n = q - 1, q = 2^m - 1$ that works with q-ary symbols. Suppose that you were to write out (in bits) all of the "guaranteed" correctable error patterns, i.e. those with symbol weight less than $(d - 1)/2$.

(a) What is the maximum binary weight of an error pattern in the "guaranteed" correctable error pattern list?

(b) What is the minimum binary weight of an error pattern that falls outside the "guaranteed" correctable error pattern list?

(c) State the main result (in one or two sentences) concerning list decoding of Reed-Solomon codes.