EE/Ma 127b Error-Correcting Codes — R. J. McEliece
draft of February 12, 2001 — 162 Moore

Homework Assignment 3 (**Final version**)
Due 9am February 16, 2001

Reading: Wicker, Chapter 8, Section 8.3
RJM "Chapter 9", Section 9.6,, pp. 18–20.

Problems to Hand In:

Problem 1. (This problem is an extension of the class discussion from Feb. 5.) Let $\mathcal{P}$ be the set of all polynomials of degree $\leq k-1$ over a finite field F with q elements, i.e., polynomials of the form

$$P(x) = I_0 + I_1 x + \cdots + I_{k-1}x^{k-1},$$

where $I_0, \ldots, I_{k-1}$ are elements of F. Now let $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \infty)$ be a list of $n+1$ distinct elements of F, including the bogus element "∞." Show that if we define $P(\infty) = I_{k-1}$, then the set of vectors of the form

$$(P(\alpha_0), P(\alpha_1), \ldots, P(\alpha_{n-1}), P(\infty))$$

is an MDS code,, i.e., an $(n+1, k)$ linear code over F with minimum (nonzero) weight $n-k+2$.

Problem 2. In class on Wednesday Feb. 7 I derived the following formula for the number of words of weight w in an (n, k) MDS code:

$$A_w = \binom{n}{w} \sum_{j=0}^{k-t-1} (-1)^j \binom{w}{j} (q^{k-t-j} - 1),$$

where $t = n - w$. Show that this formula is equivalent to that given in Theorem 8.5 of Wicker (p. 189).

Problem 3. In the "frequency domain" version of the RS Euclidean decoder, what will happen if there are no erasures and the procedure `Euclid` returns $\sigma(x) = 1$?

Problem 4. Consider ant (n, k) RS code over $GF(q)$. We say that *decoder error* has occurred if $e_0 + 2e_1 > r$, but the decoder returns a codeword differing from the (unerased positions of the) received word in e_1' positions, where $2e_1' \leq r - e_0$. Find the probability of decoder error for the $(31, 15)$ class project code when

(a) $e_0 = 16$, $e_1 = 1$.

(b) $e_0 = 15$, $e_1 = 1$.

(c) $e_0 = 14$, $e_2 = 2$¿