ENEE626. Problem set 2. Due in class on 10/15/15.

1. Given a linear code $\mathcal{C}[n,k]$ over an alphabet of size q, define a random variable X with pmf

$$P(X=i)=\frac{A_i}{q^k},\quad i=0,1,\dots,n,$$

where A_i is the coefficient of the weight distribution of $\mathcal{C}$. Prove that if $d^\perp(\mathcal{C})\geq 3$ then $EX=(q-1)n/q$ and $\mathrm{Var}(X)=n(q-1)/q^2$.

Hint: begin with the MacWilliams equation

$$A(y)=\frac{1}{q^{n-k}}A^\perp(1+(q-1)y,1-y)$$

(note a typo on the last slide of Pt.I of the notes, now corrected).

2. Construct $\mathbb{F}_{16}$ as a degree-2 extension of the field $\mathbb{F}_4$. Namely, do the following:

Let α be the primitive element of $\mathbb{F}_{16}$ that satisfies $\alpha^4=\alpha+1$.

(a) Let $\mathbb{F}_4=\{0,1,\omega,\bar{\omega}\}$. Using this notation, write out the multiplication and addition tables in $\mathbb{F}_4$. Find i such that $\omega=\alpha^i$, find j such that $\bar{\omega}=\alpha^j$. Is the answer unique?

(b) Prove that $f(x)=x^2+\omega x+1$ is irreducible over $\mathbb{F}_4$.

(c) Let β be a root of $f(x)$. What is the order of β? Is β primitive?

(d) Let $\beta=\alpha^i$. What is i?

(e) Prove that $(\beta,1)$ form a basis of $\mathbb{F}_{16}$ over $\mathbb{F}_4$. Write out coefficients of the expansion of every element in $\mathbb{F}_{16}$ in this basis. In other words, your task is to add a column to the table on p.10 of the lecture notes, Pt.II writing a representation of every element of $\mathbb{F}_{16}$ as a polynomial of degree ≤ 2 over $\mathbb{F}_4$.

3. (a) Determine the number of primitive elements of $\mathbb{F}_{32}$.

(b) Show that the polynomial $f(x)=x^5+x^2+1$ is irreducible over $\mathbb{F}_2$.

(c) Are there elements $\gamma\in\mathbb{F}_{32}$ of order 15?

Let α be a zero of $f(x)$.

(d) In the expansion $\prod_{i=0}^4(x-\alpha^i)=x^5+\alpha^{j_1}x^4+\alpha^{j_2}x^3+\alpha^{j_3}x^2+\alpha^{j_4}x+\alpha^{j_5}$ find j_1,j_2,j_3,j_3,j_4,j_5.

(e) Compute the logarithm of $\alpha^4+\alpha^3+\alpha$.

(f) Let $\gamma\in\mathbb{F}_{32}\backslash\mathbb{F}_2$. Show that γ is not a root of a polynomial of degree less than 5.

(g) Show that $1,\gamma,\gamma^2,\gamma^3,\gamma^4$ is a basis for $\mathbb{F}_{32}$ as a linear space over $\mathbb{F}_2$.

(h) What are the coordinates of α^8 with respect to the basis $1,\alpha,\alpha^2,\alpha^3,\alpha^4$?

4. (It is okay to use the computer, but please explain exactly what you do in each step).

(a) Prove that $\alpha=2$ is a primitive element of $F=\mathbf{F}_{11}$.

(b) Let C be a $[n=9,k=5]$ RS code over F with the defining set $\mathscr{P}=(\alpha,\alpha^2,\dots,\alpha^9)$ (in this order). Write out a parity-check matrix H of F.

(c) Reduce H to a systematic form $H'=[I_4|A]$.

(d) Write out the generator matrix of C in a systematic form $G=[I_5|B]$.

(e) Using H', find the codeword $\boldsymbol{c}_0$ that corresponds to the message symbols $(1,2,3,4,5)$, assuming that the encoding is systematic.