ENEE626 Problem set 3. Due in class on Thursday 11/17/2014.

1. (*The Trace Function.*) For an element $a \in \mathbb{F}_{p^m}$ define its trace as $Tr(a) = \sum_{j=0}^{m-1} a^{p^j}$. The trace function describes linear maps from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. It has many different applications. For instance, let $\mathcal{C} \in \mathbb{F}_{p^m}^n$ be a linear code and let $\mathcal{C}' := \mathcal{C}|_{\mathbb{F}_p}$ be its subfield subcode. Then $(\mathcal{C}')^\perp$ (the dual of $\mathcal{C}'$, also a code over $\mathbb{F}_p$) is equal to $Tr(\mathcal{C}^\perp)$ (the trace mapping is applied coordinate-wise). In this problem you will establish simple properties of the trace function.

(a) Prove that $Tr(a) \in \mathbb{F}_p$ for any $a \in \mathbb{F}_{p^m}$.

(b) Prove that $Tr(a+b) = Tr(a) + Tr(b)$.

(c) Prove that $Tr(\beta)$ takes every value in $\mathbb{F}_p$ equally often.

(d) Prove that $Tr(\beta^p) = Tr(\beta)^p = Tr(\beta)$.

(e) Let $g(x) = x^r + a_{r-1}x^{r-1} + \ldots$ be the minimal polynomial of $\beta \in \mathbb{F}_{p^m}$. Prove that $Tr(\beta) = -ma_{r-1}/r$.

2. (*Random linear codes.*) Consider the ensemble $\mathcal{E}(n,k)$ of all binary linear codes of length n and dimension k.

(a) Prove that a set of k linearly independent vectors in $\mathbb{F}_2^n$ can be chosen in $\prod_{j=0}^{k-1}(2^n - 2^j)$ ways.

(b) Prove that a given $[n,k]$ linear code contains $\prod_{j=0}^{k-1}(2^k - 2^j)$ different bases.

(c) Conclude that there are

$$\begin{bmatrix} n \\ k \end{bmatrix} \triangleq \prod_{j=0}^{k-1} \frac{2^{n-j}-1}{2^{k-j}-1}$$

linear codes of dimension k.

(d) Let $\boldsymbol{x} \in \mathbb{F}_2^n, \boldsymbol{x} \neq 0$. Prove that $\boldsymbol{x}$ is contained in $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ different codes from the ensemble $\mathcal{E}(n,k)$.

(e) Let $A_w(\mathcal{C})$ be the number of vectors of weight w in a code $\mathcal{C} \in \mathcal{E}(n,k)$. Suppose that the code is chosen from $\mathcal{E}(n,k)$ with uniform probability. Use the Markov inequality to prove that

$$\Pr[A_w(\mathcal{C}) \geq n\binom{n}{w}2^{k-n}] < \frac{1}{n}.$$

(f) Prove that (e) implies the existence of an $[n, k = Rn, d]$ binary linear code with weight distribution

$$A_0 = 1, A_w < n\binom{n}{w}2^{n(R-1)}, \quad 1 \leq w \leq n.$$

Prove that $\lim_{n\to\infty} \frac{d}{n} = h^{-1}(1-R)$, where $h(x)$ is the binary entropy function and h^{-1} is its inverse function.

3. (*Generator matrix ensemble.*) Let $1 \leq k < n$. Consider an ensemble of linear codes obtained by choosing a $k \times n$ generator matrix by selecting every entry independently with probability $p(0) = p(1) = 1/2$. Let $A_w, w = 0, 1, \ldots, n$ be the number of vectors of weight w in the code.

(a) Prove that

$$EA_0 = 1 + \frac{2^k - 1}{2^n}; \qquad EA_w = \binom{n}{w}\frac{2^k-1}{2^n}, \quad w \geq 1$$

$$EA_w^2 = EA_w + \frac{(2^k-1)(2^k-2)}{2^{2n}}\binom{n}{w}^2.$$

(b) Find Var $A_w, w \geq 1$. Prove that a typical code from the ensemble has distance that approaches the asymptotic GV bound as $n \to \infty$ and $k = Rn, 0 < R < 1$ (formulate the precise claim and prove it).

4. (*Erasure channel.*) Suppose that an $[n,k,d]$ binary linear code C is used for transmission over the erasure channel with erasure probability p.

(a) Maximum Likelihood decoding of the code C was defined in earlier in class, and it was explained that for the BSC, ML decoding is equivalent to decoding to the nearest codeword. What is an equivalent description of ML decoding in the case of the BEC?

(b) Let $P_e(C,p)$ be the average probability of decoding error under the ML decoding of the code C. Prove that

$$P_e(C,p) \leq \sum_{e=d}^{n-k} p^e(1-p)^{n-e}\sum_{i=d}^{e} A_i\binom{n-i}{e-i} + \sum_{e=n-k+1}^{n}\binom{n}{e}p^e(1-p)^{n-e}.$$