Course: CS 4803/8803 (Spring'08) – Homework 5

Instructor : Prasad Tetali, office: Skiles 234, email: tetali@math.gatech.edu
Office Hours: **Wed. Fri. 4:30-5:30pm, and by appointment**

Due: Wednesday, April 3rd

All problems are from Ron Roth's textbook.

Problem 1. [Problem 4.6] Show that the minimum distance of a perfect code must be odd.

Problem 2. [Problem 4.7] Let $F = \mathrm{GF}(q)$ and let n be a prime such that $\gcd(n, q) = 1$. Denote by e the multiplicative order of (the field integer) $\bar{q}$ in $\mathrm{GF}(n)$. (Recall that for a positive integer m, the element $1 + 1 + \cdots + 1$ (m times) in a field F is denoted as the Field integer $\bar{m}$, where 1 is the identity of the multiplicative group of F.)

(1). Show that there exists a perfect linear $[n, k]$ code over F only if e divides $n - k$.
Hint: Show that n divides $\mathrm{Vol}_q(n, t) - 1$ whenever $t < n$.

(2) Find all the values of k that satisfy the necessary condition of part (1) in the following two cases:
(a) $q = 2$ and $n = 23$.
(b) $q = 3$ and $n = 11$.

Problem 3. [Problem 4.14] A soccer betting form contains a list of 13 matches. Next to each listed match there are three fill-in boxes which correspond to the following three possible guesses: "first team wins," "second team wins," or "tied match." The bettor checks one box for each match.

Describe a strategy for filling out the *smallest* number of forms so that at least one of the forms contains at least 12 corrrect guesses. How many forms need to be filled out under this strategy?

Hint: Consider a perfect code of length 13 and minimum distance 3 over $\mathrm{GF}(3)$.

Problem 4. [Problem 4.19] The Hamming weight enumerator of a code $\mathcal{C}$ is the generating function,

$$W_{\mathcal{C}}(z) = \sum_{i=0}^{n} W_i z^i ,$$

where W_i equals the number of codewords in $\mathcal{C}$ of Hamming weight i.

Let $F = \mathrm{GF}(q)$ and consider transmission through a memoryless q-ary symmetric channel with crossover probability p. For a linear $[n, k, d]$ code $\mathcal{C}$ over F, let $\mathcal{D}_{\mathrm{MLD}} : F^n \to \mathcal{C}$ be a maximum-likelihood decoder for $\mathcal{C}$ with respect to this channel. Show that the decoding error probability P_{err} of $\mathcal{D}_{\mathrm{MLD}}$ is bounded from above by

$$P_{\mathrm{err}} \le W_{\mathcal{C}}\left(2\sqrt{p(1-p)/(q-1)} + (p(q-2)/(q-1))\right) - 1 .$$

Hint: Refer to Problem 1.9 done in class and in HW 4.