Math 567
Winter 2009
Carl Miller

Problem Set #6

Due date: Wednesday, April 15th.

1. Consider one of the "Hadamard codes" defined in the first paragraph of section 4.1 in van Lint. Let n be the length of the code. What is the distance distribution of the code (in terms of n)?

2. Let p be a prime and let k be a positive integer which is smaller than p. Let $\alpha \in \mathbb{F}_p$ be a multiplicative generator. Let

$$S(k) = \left\{ \left(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{p-2})\right) \mid f \in \mathbb{F}_p[X] \text{ is a polynomial of degree } < k \right\}.$$

($S(k)$ is a Reed-Solomon code.) How many codewords of weight $p-k$ does $S(k)$ contain?

3. Let p be a prime. Describe all linear codes $C \subseteq (\mathbb{F}_p)^p$ that have the property

$$(c_1, c_2, \ldots, c_p) \in C \Rightarrow (c_p, c_1, c_2, \ldots, c_{p-1}) \in C.$$

(Be explicit.)

4. Consider all subsets of $\mathbb{F}_{81}$ of the form

$$\{x^{(3^k)} \mid k = 1, 2, 3, \ldots\},$$

where x is an element of $\mathbb{F}_{81}$. What are all possible sizes for these sets? How many sets of each size exist?

(Note: Don't overcount. We consider two sets to be the same if they contain the same elements.)

5. *(Extra credit)* How many cyclic linear codes of length 13 over $\mathbb{F}_3$ exist?