Chris

Coding Theory Prelim 2006

Do as many problems as you can but you should be able to attempt at least 100 points worth in 3 hours.

1. Prove that an (n, k, d) code can correct s erasures and e errors as long as $2e + s \leq d - 1$. (20 points)

2. Find the Hensel lift of $x^4 + x + 1 \in \mathbb{Z}_2[x]$ to $\mathbb{Z}_4[x]$ which is a divisor of $x^{15} - 1 \in \mathbb{Z}_4[x]$ (10 points)

3. Let C be a linear code and $C^\perp$ its dual. Prove that $Aut(C) = Aut(C^\perp)$ where Aut is the automorphism group of permutations. (20 points)

4. Prove that the dual of an Reed-Muller code $RM(1, m)$ is the Reed -Muller code $RM(m-2, m)$. (30 points)

5. Let P_k denote all polynomials of degree $< k$ over $\mathbb{F}_q$. Define $C = \{ev(f) \in \mathbb{F}_q^n | f \in P_k\}$ where ev is the evaluation of $f(x)$ on $\mathbb{F}_q \setminus \{0\}$ and $n = q - 1$.

   (a) Prove that C is a maximum distance separable code (MDS). (20 points)

   (b) Prove that $C^\perp$ is a maximum distance separable code (MDS) given that C is MDS.(20 points)

   (c) Prove that C is a Reed-Solomon code with defining roots $\alpha^i, i = 1, 2, \ldots, d-1$ where α is a primitive element.(20 points)

6. Prove the BCH root bound on the minimum distance of a cyclic code of length $n = 2^r - 1$. (20 points)

7. Let $(g_1(D), g_2(D), \ldots, g_m(D))$ be an encoder for an $(n, 1, m)$ convolutional code. Prove that the following are equivalent(total =50 points-partial credit allowed):

   (a) The encoder is catastrophic

   (b) The $g.c.d.\{g_1, \ldots, g_m\} > 1$

   (c) the corresponding state diagram has a zero weight cycle (other than the zero loop from the zero state).

8. Let χ be the (non-singular) elliptic curve over $\mathbb{F}_2$ defined by $x^3 + xz^2 + z^3 + y^2z + yz^2 = 0$ (genus is 1). Let $D = kP_\infty$, where $P_\infty = (0 : 1 : 0)$.

   (a) Find the affine points on χ over $\mathbb{F}_8$. (20 points)

   (b) Find the intersection divisors for the curves $x = 0, y = 0, z = 0$ and $div(x^i y^j / z^{i+j})$ (20 points)

   (c) Find a basis for the AG code $L(D)$ for k=4 (20 points)