Prelim exam -Coding Theory
June 2013

You should be able to complete about 4-5 problems in 3 hours. At least one problem should involve a proof.

1. State and prove the Singleton Bound.

2. State and prove the Plotkin Bound.

3. State and prove the BCH bound. Apply it to the binary code of length 15 having defining roots $\beta^9, \beta^7 \in \mathbb{F}_{16}$ for primitive element β(i.e. all codewords having these roots).

4. A Simplex code is the dual of a Hamming code. Show that a Simplex code of length $2^r - 1$ has minimum distance 2^{r-1} and is equidistant.

5. The sequence of syndromes and its characteristic polynomial are given by the Key Equation

$$\hat{\delta}(x)S(x) = r(x) \pmod{x^{\delta-1}}$$

where $\hat{\delta}(x)$ and $r(x)$ are relatively prime and $deg(r(x)) < deg(\hat{\delta}(x))$. Given the binary sequence $S = 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1$ of length 14, use either the Euclidean Algorithm or Berlekamp-Massey Algorithm to find the characteristic polynomial $\hat{\delta}(x)$.

6. For the nonsingular Hermitian curve $\mathcal{H}_2$ over $\mathbb{F}_4$ given by

$$\chi = \{(x : y : z) | x^3 + y^2 z + yz^2 = 0\}$$

List the 8 affine $\mathbb{F}_4$-rational points. Let P be the divisor for these points. Let $P_\infty = (0 : 1 : 0)$ and $D = 3P_\infty$. Find the dimension, and a lower bound on the minimum distance of the code $C(\chi, P, D)$. Find a basis using functions $x^i y^j / z^{i+j}$. Support your answer.

7. Find the Hensel lift of the binary polynomial $1 + x + x^4$ to a monic, basic, irreducible polynomial over Z_4. Use it to construct the log table $\mathcal{T}$ with its 2-adic representation for the Galois Ring $GR(4^4)$.

8. State and prove Graeffe's Method for computing the Hensel lift of a binary polynomial.

9. Given $\alpha \in \mathbb{F}_{2^m}$ is a primitive element in the subfield of order 2^t, prove that $f(x) = \prod_{i=0}^{t-1}(x - \alpha^{2^i})$ is a binary polynomial. (i.e. the coefficients are in the binary subfield)

10. Consider a Reed-Solomon code of length 15 with roots $\beta^1, \beta^2, \beta^3, \beta^4 \in \mathbb{F}_{16}$. Suppose y is received and the Key Equation

$$r(x) = \hat{\delta}(x)S(x) \pmod{x^{\delta-1}}$$

is

$$r(x) = (1 + \beta^2 x + \beta^{14} x^2)(\beta^4 + \beta^9 x + \beta^5 x^2 + \beta^{11} x^3) \pmod{x^4}$$

. The error polynomial is $e(x) = a_4 x^4 + a_{10} x^{10}$. The residual polynomial is $r(x) = \beta^4 + \beta^5 x$. Use Forney's Algorithm to find the error values a_4, a_{10}

Table 1: Log table for $\mathbb{F}_8$ and $\mathbb{F}_{16}$

0	000
$1 = \beta^0$	100
β^1	010
β^2	001
β^3	110
β^4	011
β^5	111
β^6	101

0	0000
$1 = \beta^0$	1000
β^1	0100
β^2	0010
β^3	0001
β^4	1100
β^5	0110
β^6	0011
β^7	1101
β^8	1010
β^9	0101
β^{10}	1110
β^{11}	0111
β^{12}	1111
β^{13}	1011
β^{14}	1001