Math 422 Winter 2007 - Sample Problems

April 9, 2007

Problem 1. Let C be the linear code of length 10 over $F = \mathbb{Z}_{11}$ given by the equations $\sum_{i=1}^{10} ix_i = 0$. That is $\mathbf{x} \in F^{10}$ is a codeword if and only if $x_1 + 2x_2 + \cdots + 10x_{10} = 0$. To distinguish the symbol 10 from the sequence of symbols 1 0 we write X instead of 10.

a) Find a generator matrix for C.

b) Find a parity check matrix for C.

c) Compute the dimension of C and $C^{\perp}$.

d) Find the minimum distance of C and $C^{\perp}$. Justify your answers.

e) Suppose the vector $\mathbf{y} = X23456789X$ is received. Use syndrome decoding (with your parity check matrix in b)) to obtain a codeword. How many errors did at least occur?

f) In your answer in e), is there a unique nearest neighbour? Or could you have decoded to a different codeword which is also a nearest codeword? Justify your answer.

Problem 2. Let $F_8 = \mathbb{Z}_2[x]/\langle 1 + x + x^3 \rangle$ and denote the congruence class of x in F_8 by a.

a) Let $\alpha = 1 + a$. Find the minimal polynomial m_α of α over $\mathbb{Z}_2$. (Hint: What are the roots of m_α?)

b) Let C be the binary BCH code of length 7 and design distance $d = 5$ given by α. (You may use without proof that α has order 7.)

Find the generator polynomial of C. You do not need to multiply it out.

c) What is the dimension of C?

d) Use the factorization $x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ to identify the check polynomial for C.

e) Suppose the vector $\mathbf{y} = 1101011$ is received. Using the check polynomial from d), test whether $\mathbf{y}$ is a codeword.

f) Use the BCH decoding procedure to obtain the original codeword if possible. How many errors did occur?

Element	Power of α
0	N/A
1	α^7
a	α^5
a^2	α^3
$1 + a$	α^1
$1 + a^2$	α^2
$a + a^2$	α^6
$1 + a + a^2$	α^4

Problem 3.

a) Prove that a Hamming code is perfect. (You may use the fact that a Hamming code has minimum distance 3.)

b) Let q be a prime. Write down a PCM for a q-ary Hamming code with redundancy 2.

Problem 4. For each of the following statements indicate whether it is true or false:

a) Any binary Hamming code is equivalent to a cyclic code.

b) $R_{q,n} = F_q[x]/\langle x^n - 1\rangle$ is a field if and only if $n = 1$.

c) There is a field with 256 elements.

d) There is a field with 255 elements.

e) A standard array for a linear $[n, k, d]$-code over F_q has q^{n-k} rows.

f) Every code is equivalent to a linear code.

Problem 5. Let F_q be a finite field with q elements. Suppose $q - 1$ is prime. Show that every nonzero element of F_q is primitive.

Problem 6.

a) Show that $f = 1 + x + x^2 + x^3 + x^4$ is irreducible in $\mathbb{Z}_2[x]$.

b) Let $F_{16} = \mathbb{Z}_2[x]/\langle f\rangle$ and suppose α is a primitive element of F_{16}. What is the degree of its minimal polynomial over $\mathbb{Z}_2$.

c) What is the degree of m_{α^7}? Justify your answer.