Exam Introduction to Coding Theory code 211140

Date	:	3-04-2008
Location	:	LA 3520
Time	:	09:00-12.30

Please provide clear motivation for all your answers and indicate which theorems you are using.
Do not spend too much time on a single item. If you are not able to solve part(s) of a problem, then move on and use those parts as if you have already solved them.

There are five exercises.

1. Consider a binary memoryless channel with channel probabilities:

$$P(0 \text{ received } \mid 0 \text{ sent}) = 0.9 \quad P(1 \text{ received } \mid 1 \text{ sent}) = 0.6$$

   (a) Give the definition of a binary memoryless symmetric channel. Is the given channel symmetric?

   (b) Let $C = \{000, 100, 111\}$. One of these words was transmitted and 011 was received. Decode the received word using maximum likelihood decoding.

2. Let $f(x) \in \mathbb{F}_3[x]$ be given by $f(x) = x^4 + 2x^3 + x^2 + 2x + 1$.

   (a) Show that there does not exist a polynomial $g(x) \in \mathbb{F}_2[x]$ of degree two that divides $f(x)$. Hint: postulate that such $g(x) = x^2 + g_1x + g_0$ does exist and perform long division of $f(x)$ by $g(x)$.

   (b) Show that $f(x)$ is irreducible over $\mathbb{F}_2$.

3. (a) Determine r such that there exists a Ham$(r, 2)$ code of length 15.

   (b) Write down a parity-check matrix H for a binary Hamming code C of length 15.

   (c) Give a generator matrix G for C.

   (d) What are the dimension and minimum distance of C?

   (e) Show that C achieves the Hamming bound.

   (f) Use syndrome decoding to decode the received word 111110000011111.

4. Let C be the binary cyclic code of length 7 generated by $g(x) = (x+1)(x^3 + x^2 + 1)$.

   (a) What is the dimension of C?

   (b) Give the parity-check polynomial of C.

   (c) Write down a generator matrix G and a parity-check matrix H for C.

   (d) What is the minimum distance of C?

   (e) Show that $x^i + x^{i+1} (\mod x^7 - 1)$ and $x^j + x^{j+1} (\mod x^7 - 1)$ $(0 \leq i < j \leq 6)$ are in different cosets of C.

   (f) A codeword $c \in C$ is transmitted. During transmission two adjacent symbols were swapped resulting in a received word w. Show that although w contains two errors, it can still be decoded to c with nearest neighbour decoding.

5. Let $\alpha \in \mathbb{F}_{16}$ be a root of $1 + x^3 + x^4$.

   (a) Determine the cyclotomic cosets $C_1, \ldots, C_5$

   (b) Determine the minimal polynomials $M^{(i)}(x) \in \mathbb{F}_2[x]$ of α^i, $i = 1, \ldots 5$.

   (c) Let $g(x) = \text{lcm}(M^{(1)}(x), \ldots, M^{(5)}(x))$. Determine $g(x)$.

   Let $C \subset \mathbb{F}_2^{15}$ be the BCH code generated by $g(x)$.

   (d) Determine a generator matrix G of C.

   (e) Determine a parity check matrix H of C.

Grading:

1		2		3						4						5				
a	b	a	b	a	b	c	d	e	f	a	b	c	d	e	f	a	b	c	d	e
4	4	5	5	3	5	5	4	3	5	3	4	4	4	5	4	4	5	4	5	5

Grade: $1 + \dfrac{\text{points}}{10}$