Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

Contakt during exam:
Aslak Bakke Buan 73 55 02 89/73 59 35 20

EXAM IN TMA4185 CODING THEORY

English
Monday May 23, 2005
Time: 0900-1400

Permitted aids:
approved calculator
all printed or written aids

The grades are posted in week 24.

All answers should be explained.

K denotes the field with two elements $\{0, 1\}$.

Problem 1

Let C be the linear binary Hamming-code given by the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

a) Find a generator matrix for the code. Find the minimum distance of the code.

Given an arbitrary linear binary code D of length n, we define $D(1)$ to be the code of length $n-1$, where the codewords in $D(1)$ are obtained by taking all codewords in D with 0 in the last position, and then deleting the last position. That is :
$D(1) = \{\underline{a} = (a_1, a_2, \ldots, a_{n-2}, a_{n-1}) \in K^{n-1} \mid (a_1, a_2, \ldots, a_{n-2}, a_{n-1}, 0) \in D\}$.

b) Show that $D(1)$ is a linear code.

c) Let C be the code in part a). Find a generator-matrix for $C(1)$. What is the minimum distance of $C(1)$?

d) Decode the received word $\underline{v} = (1, 1, 0, 0, 1, 1)$, given that the code $C(1)$ is used.

Now let C be any Hamming-code.

e) Use the decoding-algorithm for Hamming-codes, to describe a decoding algorithm for $C(1)$

Now let C be an arbitrary Hamming-code with dimension k, length n and minimum-distance $d = 3$. Let $C' = C(1)$, og define a code C'' of length n as follows: Let the codewords in C'' be obtained by adding a parity bit to the codewords in C'. That is: $\underline{a} = (a_1, a_2, \ldots, a_{n-1}, a_n)$ is in C'' if and only if $(a_1, a_2, \ldots, a_{n-2}, a_{n-1})$ is in C' and $wt(\underline{a})$ is an even number.

f) Show that C'' is a linear code, and that the minimum-distance of C'' is 4.

g) Show that $k'' < k$, where k'' is the dimension of C''.

Problem 2

Let $g(x) = 1 + x^2 + x^4 + x^5$ in $K[x]$, and let $C = \langle g(x) \rangle$ be a binary cyclic code of length 15.

a) Can C correct all error-patterns of weight 2?

b) Show that C can be used to correct errors, when the error-pattern is either of the form $00\ldots0110\ldots00$ or of the form $00\ldots010\ldots00$. In other words: Show that the code is 2-error-burst correcting.

c) Decode $r = 000000010101010$, given that the code is C, and that the error-pattern is as in part b).

Problem 3

For which values of d is there a binary $[11, 8, d]$-code?

Problem 4

Let the finite field $GF(8)$ be constructed using the polynomial $x^3 + x + 1$, and let β be a primitive element in this field. Let C be the $RS(2^3, 5)$-code with generator-polynomial $g(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^3 + x)$.

a) How many errors can the code C correct?

b) Decode the received word $\underline{r} = (1,\ 0,\ \beta^5,\ \beta^2,\ 1,\ 0,\ 0)$.