NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **TMA4185 Coding Theory**

Academic contact during examination: Sverre Olaf Smalø

Phone: 73591750

Examination date: 21. May 2015

Examination time (from–to): 09:00–13:00

Permitted examination support material: C: Simple calculator and one A4-sheet with handwritten notes (yellow with the department's rubber stamp).

Language: English

Number of pages: 2

Number pages enclosed: 0

Checked by:

Date Signature

Problem 1 Let C be a $[13, 10, 3]$ Hamming code ($q = 3, r = 3$). Find a parity check matrix for C.

Problem 2 Binary Reed-Muller-codes. Define inductively the codes $R(r, m)$ with $0 \leq r \leq m$ of length 2^m by the generating matrices $G(r, m)$ given by

i. $G(0, m)$ is the 1×2^m-matrix $(11 \ldots 1)$,

ii. $G(m, m)$ is the $2^m \times 2^m$-identity matrix and

iii. for $0 < r < m$ is

$$G(r, m) = \begin{pmatrix} G(r, m-1) & G(r, m-1) \\ 0 & G(r-1, m-1) \end{pmatrix}$$

a) Prove that for $0 \leq i \leq j \leq m$, $R(i, m) \subseteq R(j, m)$.

b) Prove that the dimension of $R(i, m) = \binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{i}$.

c) Prove that the minimal distance in $R(r, m)$ is 2^{m-r}.

d) Prove that $R(m, m)^{\perp} = 0$ and that for $0 \leq r < m$, $R(r, m)^{\perp} = R(m - r - 1, m)$.

Problem 3 For each prime power q and natural number n, let $A_q(n, d)$ be the maximal number of elements in a code C in F_q^n where the distance between different code words in C is at least d.

Prove that:

i. $A_q(n, n) = q$,

ii. $A_q(n, d) \leq qA_q(n-1, d)$ when $0 \leq d < n$ and that

iii. $A_q(n, d) \leq q^{n-d+1}$.

Problem 4 How many cyclic codes of length 63 exists over F_2?.

Problem 5 Consider the 2×4-matrix

$$G = \begin{pmatrix} 1 & 1+D+D^2 & 1+D & 1+D \\ 0 & 1+D & D & 1 \end{pmatrix} \tag{1}$$

and let G be a generator matrix for a convolution code.

a) What is the exterior degree and what is the internal degree of G?

b) Is G a cannonical matrix? You have to give a reason for your answer.

c) Draw a linear feed-forward shift-register which implements the encoding with G, and encode the pair $(1101, 1001)$ of sequences by starting from the left where the pair of sequences represents the pair $(1 + D + D^3, 1 + D^3)$ of polynomials.