NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **TMA4185 Coding Theory**

Academic contact during examination: Sverre O. Smalø

Phone: 7359 1750

Examination date: Mai 19th 2014

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

Permitted examination support material: B: All printed and hand written documents allowed. Simple approved calculator allowed.

Language: English

Number of pages: 1

Number pages enclosed: 0

Checked by:

12.05.14 Elen Haagensen

Date Signature

Problem 1 Consider the field $F_{17} = \mathbb{Z}_{17}$ with 17 elements.

a) Find a primitive element for F_{17}.

b) Construct by finding the generating polynomial of the narrow sense Reed-Solomon code for F_{17} with defined distance 7 based on your primitive element.

Problem 2 Let $F_2 = \mathbb{Z}_2$ be the field with 2 elements.

a) How many irreducible factors has $X^{63} + 1$ in $F_2[X]$ and how many cyclic codes of length 63 exist over F_2.

Problem 3 Let $F_2 = \mathbb{Z}_2$ be the field with two elements and consider the convolutional code C in $F_2(D)^2$ given by the encoding matrix

$$M = (D^5 + D^4 + 1 \quad D^3 + 1).$$

a) Show that the matrix M is reduced but not basic.

b) Find a canonical generator matrix for the code C, and construct a linear feedforward shift-register to implement the encoding using the canonical generator matrix.

c) Draw a state diagram for the encoding with the canonical matrix for the code C, and encode the sequence 100111.

Problem 4 Let p be a prime number, $F_p = \mathbb{Z}_p$ the field with p elments, and $g = g_0 + g_1X + g_2X^2 + \cdots + X^n$ a monic irreducible polynomial of degree $n \geq 3$ in $F_p[X]$.

a) Prove that if α is a root of g in an extension field F_q of F_p, then so is α^p.

b) Prove that $g = \prod_{i=0}^{n-1}(X - \alpha^{p^i})$.

c) Let $h = (1/g_0)(X^n g(1/X))$ be the reciprocal polynomial of g. Prove that h is also irreducible with roots $\alpha^{-(p^i)}$ for $i = 0, 1, \cdots n-1$.

d) Prove that if $h = g$, then the order of α is properly less than $p^n - 1$ by using that $n \geq 3$.