NTNU

Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **TMA4185 Coding theory**

Academic contact during examination: Kristian Gjøsteen
Phone: 73 55 02 42

Examination date: May 15, 2017

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

Permitted examination support material: All printed and hand-written support material is allowed. A specific basic calculator is allowed.

Other information:

Language: English

Number of pages: 2

Number of pages enclosed: 0

Checked by:

4/5-17 [signature]

Date Signature

Informasjon om trykking av eksamensoppgave	
Originalen er:	
1-sidig ☒	**2-sidig** ☐
sort/hvit ☒	**farger** ☐
skal ha flervalgskjema ☐	

Problem 1 Consider the linear code over $\mathbb{F}_3$ defined by the parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 2 & 2 \\ 1 & 1 & 0 \end{bmatrix}.$$

a) Find a generator matrix for the code. What is the code's dimension? How many code words are there in the code?

b) What is the code's minimum distance d? How many errors can the code correct? How many errors can the code detect?

c) You have received $\vec{y} = (1, 2, 0, 0, 2, 1)$. If there are at most $(d-1)/2$ errors, what is the error vector?

d) Let $\hat{C}$ be the code C extended by adding a parity check symbol ensuring that for every code word the sum of its coordinates is zero (it is *even-like*):

$$\hat{C} = \left\{ (c_1, c_2, \ldots, c_7) \in \mathbb{F}_3^7 \;\middle|\; (c_1, c_2, \ldots, c_6) \in C \wedge \sum_{i=1}^{7} c_i = 0 \right\}.$$

Give a generator matrix and a parity check matrix for $\hat{C}$. What is the dimension of $\hat{C}$?

What is the minimum distance of $\hat{C}$.

Problem 2 Let C be a linear code over the field $\mathbb{F}_q$, and consider the first coordinate of the code words. Prove that either every code word has 0 in its first coordinate, or exactly $1/q$ of all code words have 0 in their first coordinate.

Problem 3 Let $\omega \in \mathbb{F}_4$ have the property that $\omega^2 = \omega + 1$. Consider the convolutional code over $\mathbb{F}_4$ given by $G = (x + 1 \quad x^2 + x + \omega)$.

Encode the message $0, 1, \omega, \omega + 1, 0, 1, \omega, \omega + 1, 0, 0, 0, 0$.

Problem 4 Let $\beta \in \mathbb{F}_{16}$ satisfy $\beta^4 = \beta + 1$. Let C be the Reed-Solomon code of length 15 with the twelve zeros $\{1, 2, 3, \ldots, 12\}$ and generator polynomial

$$\begin{aligned} g(x) = \beta^3 &+ \left(\beta^3 + \beta^2 + 1\right) x + \left(\beta^3 + \beta^2\right) x^2 + \beta^2 x^3 + \left(\beta^3 + 1\right) x^4 \\ &+ \left(\beta^3 + \beta^2 + 1\right) x^5 + \beta^2 x^6 + x^7 + \beta^3 x^8 + \left(\beta^2 + 1\right) x^9 \\ &+ \left(\beta^3 + 1\right) x^{10} + \left(\beta^2 + 1\right) x^{11} + x^{12}. \end{aligned}$$

a) How many errors can the code correct? How many erasures can the code correct? What is the dimension of the code?

Can you find a linear code of the same length with the same minimum distance over the same field, but with higher dimension?

b) A message has been encoded as $m(x)g(x)$. You receive

$$y(x) = \beta^3 + \left(\beta^3 + \beta^2 + \beta\right) x + \left(\beta^3 + \beta^2 + 1\right) x^2$$

where all the other coefficients have been erased. Recover the encoded message $m(x)$.

Problem 5 In this problem we will consider cyclic codes of length 9 over $\mathbb{F}_2$.

It may be useful to know that 9 divides $2^6 - 1$, that $x^6 + x^3 + 1$ is irreducible over $\mathbb{F}_2$ and that there is an element α in $\mathbb{F}_{64}$ with order 9 satisfying $\alpha^6 = \alpha^3 + 1$.

a) Describe all such cyclic codes. For each code, give a generating polynomial and determine the minimum distance.

b) Consider the code with generating polynomial $g(x) = x^6 + x^3 + 1$. Suppose you received

$$y(x) = x^8 + x^6 + x^5 + x^3 + x^2 + x + 1$$

and there is exactly one error. Find the location of the error and the correct code word.