MTAT.05.082: Introduction to Coding Theory **University of Tartu**

Final exam

Instructors: Dr. Vitaly Skachek, Yauhen Yakimenka June 8th, 2015

Student name: ____

Student ID: ____

1. This exam contains 10 pages. Check that no pages are missing.
2. It is possible to collect up to 110 points. Try to collect as many points as possible.
3. Justify and prove all your answers.
4. All facts and results that were proved or stated in the class can be used in your solution without a proof. Such results need to be rigorously formulated.
5. Any printed and written material is allowed in the class. No electronic devices are allowed.
6. Exam duration is 3 hours.
7. Good luck!

Question 1	
Question 2	
Question 3	
Question 4	
Total	

Question 1 (20 points).

A code $\mathcal{C}$ is defined as the following set of vectors over $\mathbb{F}_3$

$$\mathcal{C} = \{\mathbf{c} \mid \boldsymbol{K}\mathbf{c}^\intercal = \mathbf{0}^\intercal\} ,$$

where

$$\boldsymbol{K} = \begin{pmatrix} 0 & 1 & 2 & 0 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 2 \end{pmatrix} .$$

(a) What is the length n, dimension k and minimum distance d of the code $\mathcal{C}$?

(b) Find a generator matrix of the code $\mathcal{C}$.

Question 2 (30 points).

Let $\mathcal{C}$ be an MDS $[n, k, d]$ code over the finite field $\mathbb{F}$. Denote by $\boldsymbol{H}$ the $(n-k) \times n$ parity-check matrix of $\mathcal{C}$.

(a) Let $\boldsymbol{H}_1$ be a matrix obtained from $\boldsymbol{H}$ by removing *one* of its *columns*. Show that $\boldsymbol{H}_1$ is a parity-check matrix of an MDS $[n-1, k-1, d]$ code over $\mathbb{F}$.

(b) Show that there exists a parity-check matrix $\boldsymbol{H}'$ of $\mathcal{C}$ of the following form:

$$\boldsymbol{H}' = (\, \boldsymbol{I} \mid \boldsymbol{A} \,) \,,$$

where $\boldsymbol{I}$ is the $(n-k) \times (n-k)$ identity matrix, and $\boldsymbol{A}$ is an $(n-k) \times k$ matrix, both over $\mathbb{F}$.

(c) Let $\boldsymbol{H}_2$ be a matrix obtained from $\boldsymbol{H}$ by removing *one* of its *rows*. Is it always true that $\boldsymbol{H}_2$ is a parity-check matrix of an MDS $[n, k+1, d-1]$ code over $\mathbb{F}$? If yes – prove, otherwise show a counterexample or explain.

Question 3 (30 points).

Let $\mathbb{F}$ be a finite field with q elements and $\mathcal{C}$ be an $[n, k, d]$ code over $\mathbb{F}$. Consider a matrix $\boldsymbol{M}$ over $\mathbb{F}$, whose rows are all the codewords of the dual code $\mathcal{C}^{\perp}$.

(a) How many rows does $\boldsymbol{M}$ have? Justify your answer.

(b) Show that if $d \geq 2$, then each symbol $a \in \mathbb{F}$ appears in column ℓ of $\boldsymbol{M}$ exactly q^{n-k-1} times, for $\ell \in \{1, 2, \cdots, n\}$.

(c) Fix any $d-1$ columns of $\boldsymbol{M}$ and call a matrix composed of these columns $\boldsymbol{M}'$. Show that for any vector $\boldsymbol{a} = (a_1, a_2, \ldots, a_{d-1}) \in \mathbb{F}^{d-1}$, there are exactly $q^{n-k-d+1}$ rows in $\boldsymbol{M}'$ equal to $\boldsymbol{a}$.

Question 4 (30 points).

Let $\mathbb{F} = \mathbb{F}_7$ be a field of integer residues modulo 7. Suppose that $\mathcal{C}$ is a $[6, 2, 5]$ Reed-Solomon code over $\mathbb{F}$, with a parity-check matrix of the code given by

$$\boldsymbol{H} = \begin{pmatrix} 2 & 2 & 3 & 3 & 4 & 4 \\ 2 \cdot 1 & 2 \cdot 2 & 3 \cdot 3 & 3 \cdot 4 & 4 \cdot 5 & 4 \cdot 6 \\ 2 \cdot 1^2 & 2 \cdot 2^2 & 3 \cdot 3^2 & 3 \cdot 4^2 & 4 \cdot 5^2 & 4 \cdot 6^2 \\ 2 \cdot 1^3 & 2 \cdot 2^3 & 3 \cdot 3^3 & 3 \cdot 4^3 & 4 \cdot 5^3 & 4 \cdot 6^3 \end{pmatrix} .$$

This means that the code locators are $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 3$, $\alpha_4 = 4$, $\alpha_5 = 5$, $\alpha_6 = 6$, and the column multipliers are $v_1 = 2$, $v_2 = 2$, $v_3 = 3$, $v_4 = 3$, $v_5 = 4$, $v_6 = 4$.

Assume that $\mathbf{c} \in \mathbb{F}^6$ is transmitted, and $\mathbf{y} = (0, 1, 2, 5, 6, 3) \in \mathbb{F}^6$ is received. In this question, you will decode $\mathbf{y}$.

(a) Find the syndrome polynomial $S(x)$.

(b) Find the error-locator and the error-evaluator polynomials by either Peterson-Gorenstein-Zierler method or by Euclid's algorithm.

(c) What are the error locations and error values?

(d) What is $\mathbf{c}$ if we assume that there were at most $\lfloor (d-1)/2 \rfloor$ errors?