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

# Final exam

Instructors: Vitaly Skachek, Yauhen Yakimenka January 24th, 2018

---

**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 $\mathbb{F}_3 = \{0, 1, 2\}$:

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

where

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

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

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

**Question 2** (30 points).

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be linear codes of the same length $n$ over the finite field $\mathbb{F}_3 = \{0, 1, 2\}$, such that $\mathcal{C}_1 \cap \mathcal{C}_2 = \{\bar{\mathbf{0}}\}$. Let $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ be parity-check matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Define the code

$$\mathcal{C}_3 = \{ \ ( \ \bar{\boldsymbol{x}} + \bar{\boldsymbol{y}} \mid \bar{\boldsymbol{x}} + 2 \cdot \bar{\boldsymbol{y}} \ ) \ : \ \bar{\boldsymbol{x}} \in \mathcal{C}_1 \text{ and } \bar{\boldsymbol{y}} \in \mathcal{C}_2 \}$$

of length $n$. For $i = 1, 2, 3$, let $k_i \geq 1$ be the dimension of $\mathcal{C}_i$ and $d_i$ be its minimum distance.

(a) Show that the code $\mathcal{C}_3$ is linear.

(b) Show that $k_3 = k_1 + k_2$.

(c) Show that

$$\boldsymbol{H}_3 = \left( \begin{array}{c|c} \boldsymbol{H}_1 & \boldsymbol{H}_1 \\ \hline -\boldsymbol{H}_2 & \boldsymbol{H}_2 \end{array} \right)$$

is a parity-check matrix of $\mathcal{C}_3$.

(d) Is it true that $d_3 \geq \max\{d_1, d_2\}$? If yes – prove, otherwise – disprove or show a counterexample.

**Question 3** (30 points).

Let $\mathcal{C}$ be an MDS $[n, k, d]$ code over the finite field $\mathbb{F}$. Denote by

$$\boldsymbol{H} = \begin{pmatrix} h_{1,1} & h_{1,2} & h_{1,3} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & h_{2,3} & \cdots & h_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1} & h_{n-k,2} & h_{n-k,3} & \cdots & h_{n-k,n} \end{pmatrix}$$

an $(n-k) \times n$ parity-check matrix of $\mathcal{C}$.

(a) Let $\boldsymbol{H}_1$ be a parity-check matrix that is obtained by adding an *arbitrary column* (of length $n-k$) to $\boldsymbol{H}$. Is it always true that $\boldsymbol{H}_1$ is a parity-check matrix of an $[n+1, k+1, d]$ MDS code over $\mathbb{F}$? If yes – prove, otherwise show a counterexample or explain.

(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 replacing one of its entries $h_{i,j}$ by zero. Is it always true that $\boldsymbol{H}_2$ is a parity-check matrix of an MDS code over $\mathbb{F}$ with minimum distance $\geq d-1$? If yes – prove, otherwise show a counterexample or explain.

(d) Let $\boldsymbol{H}_3$ be a parity-check matrix that is obtained by removing any $t$ columns from $\boldsymbol{H}$, $t < d$. Is it always true that $\boldsymbol{H}_3$ is a parity-check matrix of an MDS code over $\mathbb{F}$? If yes – prove, otherwise show a counterexample or explain.

(e) Let $\boldsymbol{H}_4$ be a parity-check matrix that is obtained by removing any $t$ rows from $\boldsymbol{H}$, $t < n-k$. Is it always true that $\boldsymbol{H}_4$ is a parity-check matrix of an MDS code over $\mathbb{F}$? If yes – prove, otherwise show a counterexample or explain.

**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

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

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 $v_1 = v_3 = v_5 = 1$ and $v_2 = v_4 = v_6 = 4$.

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

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

(e) Compute $\boldsymbol{H} \cdot \bar{\boldsymbol{c}}^T$ and show that indeed $\bar{\boldsymbol{c}} \in \mathcal{C}$.