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

Final exam

Instructors: Vitaly Skachek, Eldho K. Thomas January 3rd, 2020

Student name: _____

Student ID: _____

1. This exam contains 10 pages. Check that no pages are missing.
2. It is possible to collect up to 120 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 (30 points).

Consider the following two 3×4 parity-check matrices:

$$\mathcal{H}_1 = \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{pmatrix} \qquad \text{and} \qquad \mathcal{H}_2 = \begin{pmatrix} 1 & 3 & 0 & 3 \\ 0 & 1 & 3 & 0 \\ 1 & 0 & 1 & 3 \end{pmatrix} ,$$

that correspond to the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, respectively.

(a) Do these matrices correspond to the same code or to two different codes?

(b) What is the length n, dimension k and minimum distance d of each of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$?

Prove your answers.

Question 2 (30 points).

Definition: Let $\boldsymbol{A}$ be an $k_A \times n_A$ matrix over the finite field $\mathbb{F}$ given by:

$$\boldsymbol{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n_A} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n_A} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k_A,1} & a_{k_A,2} & a_{k_A,3} & \cdots & a_{k_A,n_A} \end{pmatrix} .$$

Let $\boldsymbol{B}$ be an $k_B \times n_B$ matrix over $\mathbb{F}$. Then, *the Kronecker product* $\boldsymbol{A} \otimes \boldsymbol{B}$ is the $k_A k_B \times n_A n_B$ block matrix:

$$\boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{1,1} \cdot \boldsymbol{B} & a_{1,2} \cdot \boldsymbol{B} & a_{1,3} \cdot \boldsymbol{B} & \cdots & a_{1,n_A} \cdot \boldsymbol{B} \\ a_{2,1} \cdot \boldsymbol{B} & a_{2,2} \cdot \boldsymbol{B} & a_{2,3} \cdot \boldsymbol{B} & \cdots & a_{2,n_A} \cdot \boldsymbol{B} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k_A,1} \cdot \boldsymbol{B} & a_{k_A,2} \cdot \boldsymbol{B} & a_{k_A,3} \cdot \boldsymbol{B} & \cdots & a_{k_A,n_A} \cdot \boldsymbol{B} \end{pmatrix} ,$$

where $a_{i,j} \cdot \boldsymbol{B}$ is a standard scalar-matrix multiplication.

Example: Take two matrices over $\mathbb{F}_3 = \{0, 1, 2\}$:

$$\boldsymbol{A} = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} \qquad \text{and} \qquad \boldsymbol{B} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} .$$

Then,

$$\boldsymbol{A} \otimes \boldsymbol{B} = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{array}\right) .$$

Tasks: Let $\mathcal{C}_A$ and $\mathcal{C}_B$ be two linear codes over $\mathbb{F}$ with parameters $[n_A, k_A, d_A]$ and $[n_B, k_B, d_B]$, and with generator matrices $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively. Let $\boldsymbol{A} \otimes \boldsymbol{B}$ be a generator matrix of an $[n, k, d]$ code $\mathcal{C}$ (after possible removal of linearly-dependent rows).

(a) Prove that $k = k_A \cdot k_B$ (Hint: it can be convenient to choose $\boldsymbol{A}$ in a systematic form – why it is always possible?)

(b) Show that $d \leq d_A \cdot d_B$.

Question 3 (30 points).

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

$$\boldsymbol{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \alpha_3^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix},$$

   where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all distinct nonzero elements in $\mathbb{F}$.

   Consider the code $\mathcal{C}'$, whose parity-check matrix is

$$\boldsymbol{H}' = \left(\begin{array}{ccccc|c} 1 & 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n & 0 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \alpha_3^{n-k-1} & \cdots & \alpha_n^{n-k-1} & 0 \end{array}\right)$$

   over $\mathbb{F}$. Prove that $\mathcal{C}'$ has parameters $[n+1, k+1, d]$. Explain why $\mathcal{C}'$ is MDS.

2. Consider the code $\mathcal{D}$, whose **generator** matrix over $\mathbb{F}$ is $\boldsymbol{H}'$ as above. What are the parameters of $\mathcal{D}$? Show that $\mathcal{D}$ is MDS.

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 given by

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

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 $v_2 = v_4 = v_6 = 6$.

Assume that $\bar{\boldsymbol{c}} \in \mathcal{C}$ is transmitted, and $\bar{\boldsymbol{y}} = (1, 5, 2, 3, 4, 6) \in (\mathbb{F})^6$ 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 $\bar{\boldsymbol{c}} \in \mathcal{C}$.