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

Final exam

Instructors: Vitaly Skachek, Eldho K. Thomas January 17th, 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 4×5 parity-check matrices:

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

that correspond to the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_2$, 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 Σ be an alphabet with q symbols, and let s and n be integers, where $1 \leq s \leq q-1$. A code $\mathcal{C}$ is called an *s-symbol code of length n over Σ* if codewords in $\mathcal{C}$ are all vectors of length n consisting of at most s different symbols.

Example: for $\Sigma = \{1, 2, 3\}$, $s = 2$ and $n = 3$, an s-symbol code is the following set of vectors:

$$\begin{aligned} \mathcal{C} \;=\; \{&(111), (222), (333), \\ &(211), (121), (112), (122), (212), (221), \\ &(311), (131), (113), (133), (313), (331), \\ &(322), (232), (223), (233), (323), (332)\} \; . \end{aligned}$$

Let $\mathcal{C}$ be an s-symbol code of length n over an alphabet Σ, $|\Sigma| = q$.

(a) What is the cardinality of $\mathcal{C}$ for $s = 1$?

(b) What is the cardinality of $\mathcal{C}$ for $s = 2$? How many codewords contain only a single symbol? How many codewords contain exactly two different symbols?

(c) Define a sphere of radius r, $0 \leq r \leq n$, around a codeword $\boldsymbol{c} \in \mathcal{C}$ as

$$\mathbb{S}_r(\boldsymbol{c}) = \{\boldsymbol{x} \;:\; \boldsymbol{x} \in \Sigma^n \text{ and } \mathsf{d}_H(\boldsymbol{c}, \boldsymbol{x}) \leq r\} \; ,$$

where $\mathsf{d}_H(\cdot, \cdot)$ denotes the Hamming distance between the two arguments.

Let $s = 1$. What is the size of $\mathbb{S}_r(\boldsymbol{c})$ for $0 \leq r \leq n$?

(d) Let $s = 1$. What is the minimum Hamming distance of an s-symbol code $\mathcal{C}$ of length n over Σ, $|\Sigma| = q$?

(e) For $s = 1$, formulate an analogue of the sphere-packing (Hamming) bound on the size of an s-symbol code $\mathcal{C}$ of length n over Σ, $|\Sigma| = q$.

(f) Is the sphere-packing bound in (e) attained with equality?

Question 3 (30 points).

Let $\mathcal{C}$ be an $[n, k, d]$ code over a finite field $\mathbb{F}$ with q elements. Denote its orthogonal code by $\mathcal{C}^{\perp}$. Let $\boldsymbol{H}$ be a $(n-k) \times n$ parity-check matrix of $\mathcal{C}$.

(a) Is it true that any $d-1$ columns of $\boldsymbol{H}$ are linearly independent? Justify your answer.

(b) Let $\boldsymbol{c} = (c_1 c_2 \cdots c_n) \in \mathcal{C}^{\perp}$ be a codeword of the dual code of $\mathcal{C}$. Select a subset $\mathcal{S} = \{i_1, i_2, \cdots, i_{d-1}\}$ of coordinates, $\mathcal{S} \subseteq \{1, 2, \cdots, n\}$. Show that any combination of $d-1$ symbols in positions $\mathcal{S}$ is possible.

(c) Assume that a codeword $\boldsymbol{c}$ is chosen from $\mathcal{C}^{\perp}$ uniformly at random. Show that for any $\mathcal{S}$ as above, any combination of $d-1$ symbols in positions $\mathcal{S}$ appears with equal probability.

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

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

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 $v_1 = v_2 = 1$, $v_3 = v_4 = 2$, and $v_5 = v_6 = 3$.

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