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

Final exam

Instructors: Vitaly Skachek, Yauhen Yakimenka December 14th, 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).

Consider the following two 3×4 matrices:

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

that generate codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_3 = \{0, 1, 2\}$, respectively.

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

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

Prove your answers.

Question 2 (30 points).

Definition: let n be an even integer. A binary (not necessarily linear) code $\mathcal{C}$ is said to be *balanced* if any codeword has equal number of zeros and ones.

Example: for $n = 4$, a code that is formed by *any nonempty subset* of the following set of vectors is balanced:

$$\{(0011), (0101), (1001), (0110), (1010), (1100)\} \ .$$

In what follows, assume that $\mathcal{C}$ is a balanced code.

(a) What is the maximal possible size of $\mathcal{C}$?

(b) Show that the Hamming distance between any two codewords in $\mathcal{C}$ is even.

(c) Define a "balanced sphere" of radius $2r$, $0 \leq r \leq n/2$, around the codeword $\bar{\boldsymbol{x}} \in \mathcal{C}$ as

$$\mathbb{S}_{2r}(\bar{\boldsymbol{x}}) = \{\bar{\boldsymbol{y}} \ : \ \bar{\boldsymbol{y}} \text{ has equal number of zeros and ones, and } \mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \leq 2r\} \ ,$$

where $\mathsf{d}_H(\cdot, \cdot)$ denotes the Hamming distance. What is the size of $\mathbb{S}_{2r}(\bar{\boldsymbol{x}})$?

(d) Let d be an integer, $1 \leq d \leq n/2$. By using the results in (a) and (c), formulate and prove a variation of a sphere-packing bound on the size of a balanced code $\mathcal{C}$ of length n with an additional property that for any two codewords $\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}} \in \mathcal{C}$, $\mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \geq 2d$.

(e) Check that your result in part (a) is a special case of the bound in part (d) (for $r = 0$).

Question 3 (30 points).

(a) Consider a linear $[n, k = n - r, d]$ code over a finite field $\mathbb{F}$ defined by a parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{n-1}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{r-2} & \alpha_2^{r-2} & \dots & \alpha_{n-1}^{r-2} & 0 \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_{n-1}^{r-1} & 1 \end{pmatrix},$$

where $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ are distinct nonzero elements of $\mathbb{F}$.

Prove that the code $\mathcal{C}$ is MDS.

(b) Prove that there exists a generator matrix of the code $\mathcal{C}$ of the following form:

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{n-1}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \dots & \alpha_{n-1}^{k-2} & 0 \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_{n-1}^{k-1} & 1 \end{pmatrix} \cdot \begin{pmatrix} u_1 & & & 0 \\ & u_2 & & \\ & & \ddots & \\ 0 & & & u_n \end{pmatrix},$$

where $u_1, u_2, \cdots, u_n$ are nonzero elements of $\mathbb{F}$.

Hint: it was shown in the class that the dual of a GRS code is a GRS code. You can use that fact.

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

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

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