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

Final exam

Instructor: Dr. Vitaly Skachek June 10th, 2014

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 (15 points). Let $\mathcal{C}$ be an $[n, k, d]$ code over $\mathbb{F}_2$, defined by the following parity-check matrix:

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

What are the values of n, k and d? Justify your answer.

Question 2 (25 points).

Definition: let w and n be integers, $0 \leq w \leq n$. A code $\mathcal{C}$ is called a *code of constant weight w and of length n over $\mathbb{F}_2$* if all vectors in $\mathcal{C}$ are binary vectors of length n having Hamming weight w.

Example: for $w = 3$ and $n = 4$, a code that is formed by *any nonempty subset* of the following set of vectors is a constant weight code:

$$\{(0111), (1011), (1101), (1110)\} \ .$$

Let $\mathcal{C}$ be a code of constant weight w and of length n over $\mathbb{F}_2$.

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

(b) Show that for any two codewords $\bar{\boldsymbol{x}}$ and $\bar{\boldsymbol{y}}$ in $\mathcal{C}$, the Hamming distance $\mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}})$ is even.

(c) Define a sphere of radius $r > 0$ around the codeword $\bar{\boldsymbol{x}} \in \mathcal{C}$ as

$$\mathbb{S}_r(\bar{\boldsymbol{x}}) = \{\bar{\boldsymbol{y}} \ : \ \mathsf{w}_H(\bar{\boldsymbol{y}}) = w \text{ and } \mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \leq r\} \ ,$$

where $\mathsf{w}_H(\bar{\boldsymbol{y}})$ denotes the Hamming weight of $\bar{\boldsymbol{y}}$. What is the size of $\mathbb{S}_r(\bar{\boldsymbol{x}})$?

(d) Let d be an integer, $1 \leq d \leq n$. By using the results in (a) and (c), formulate and prove an upper bound on the size of a code $\mathcal{C}$ of constant weight w and of length n over $\mathbb{F}_2$ with an additional property that for any two codewords $\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}} \in \mathcal{C}$, $\mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \geq d$.

Question 3 (35 points). Let $\mathbb{F}$ be a finite field with q elements, and let $\mathcal{C}$ be an $[n, k, d]$ Reed-Solomon code over $\mathbb{F}$, $q > n$.

(a) Let $\alpha_1, \alpha_2, \cdots, \alpha_k$ be elements in $\mathbb{F}$, and let $i_1, i_2, \cdots, i_k$ be a subset of k different indices from $\{1, 2, \cdots, n\}$. Show that there exists a *unique* codeword $\bar{\boldsymbol{c}} = (c_1, c_2, \cdots, c_n)$ in $\mathcal{C}$ such that $c_{i_1} = \alpha_1$, $c_{i_2} = \alpha_2$, ..., $c_{i_k} = \alpha_k$.

(b) Let t be an integer, $1 \leq t \leq k$. Let $\alpha_1, \alpha_2, \cdots, \alpha_t$ be elements in $\mathbb{F}$, and let $i_1, i_2, \cdots, i_t$ be a subset of t different indices from $\{1, 2, \cdots, n\}$. How many codewords $\bar{\boldsymbol{c}} = (c_1, c_2, \cdots, c_n)$ in $\mathcal{C}$ satisfy that $c_{i_1} = \alpha_1$, $c_{i_2} = \alpha_2$, ..., $c_{i_t} = \alpha_t$? Justify your answer.

(c) How many codewords in $\mathcal{C}$ have zeros in the first $k - 1$ coordinates?

(d) How many codewords of Hamming weight d does the code $\mathcal{C}$ have?

Question 4 (35 points).

Let $\mathbb{F} = \mathbb{F}_8$ be an extension field of $\mathbb{F}_2$ constructed using irreducible polynomial $x^3 + x + 1$, and let β be a primitive element in $\mathbb{F}$. Suppose that $\mathcal{C}$ is a $[5, 3, 3]$ Reed-Solomon code over $\mathbb{F}$, with a parity-check matrix given by

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

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

1. Find the syndrome polynomial $s(x)$.
2. Find the error-locator and the error-evaluator polynomials. Show all intermediate steps in your algorithm.
3. What are the locations and the values of the errors?
4. What is $\bar{\boldsymbol{c}}$ if there was at most one error?