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

Final exam

Instructors: Vitaly Skachek, Yauhen Yakimenka December 28th, 2016

Student name: _____

Student ID: _____

1. This exam contains 11 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 (20 points).

A code $\mathcal{C}$ is defined as the following set of vectors over $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$:

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

where

$$\boldsymbol{H} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 3 & 3 \\ 0 & 0 & 0 & 4 & 4 \end{pmatrix} .$$

(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 $\mathcal{C}$.

Solution:

(a)
- The length is obviously $n = 5$.
- The rows of $\boldsymbol{H}$ are linearly independent since the matrix is in upper-triangular form. Therefore, $n - k = 4$, or $k = 1$.
- Any two columns in $\boldsymbol{H}$ are linearly independent (because, for example, each column has a different pattern of zeros). Therefore, the minimum distance $d \geq 3$. Now, let us verify that $d \leq 3$. Denote the columns of $\boldsymbol{H}$ as $\bar{\boldsymbol{h}}_1, \bar{\boldsymbol{h}}_2, \cdots, \bar{\boldsymbol{h}}_5$. Then, it is straightforward to see that

$$\bar{\boldsymbol{h}}_1 + \bar{\boldsymbol{h}}_5 = \bar{\boldsymbol{h}}_4 \ ,$$

or

$$\bar{\boldsymbol{h}}_1 + \bar{\boldsymbol{h}}_5 - \bar{\boldsymbol{h}}_4 = \bar{\boldsymbol{h}}_1 + 4\bar{\boldsymbol{h}}_4 + \bar{\boldsymbol{h}}_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} .$$

In other words, it holds $(1\ 0\ 0\ 4\ 1) \in \mathcal{C}$, and so indeed $d \leq 3$.
We conclude that $d = 3$.

(b) Since $k = 1$, the generator matrix of $\mathcal{C}$ has only one row. It is enough to take any non-zero codeword. From (a), for example

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 4 & 1 \end{bmatrix}$$

is a generator matrix.

Question 2 (30 points).

Definition: An (n, M, d) code $\mathcal{C}$ over $\mathbb{F} = \mathbb{F}_q$, $q = n$, is called a *permutation code* if each codeword in $\mathcal{C}$ has n different symbols from $\mathbb{F}$. (Please note that the code is generally non-linear.)

Example: for $n = 3$, $\mathbb{F} = \mathbb{F}_3 = \{0, 1, 2\}$, the following code is a permutation code of Hamming distance 3:

$$\{(012), (201), (120)\} \ .$$

Let $\mathcal{C}$ be a permutation code of length n over $\mathbb{F}$.

(a) Show that for any two codewords $\bar{\boldsymbol{x}}$ and $\bar{\boldsymbol{y}}$ in $\mathcal{C}$, $\bar{\boldsymbol{x}} \neq \bar{\boldsymbol{y}}$, the Hamming distance $\mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \geq 2$.

(b) What is the maximal possible size of $\mathcal{C}$ for $d = 2$?

(c) Let $\bar{\boldsymbol{x}} \in \mathcal{C}$. Show that the maximal possible number of codewords in $\mathcal{C}$ at the Hamming distance at most $r = 2$ from $\bar{\boldsymbol{x}}$ is

$$1 + \binom{n}{2} \ .$$

(d) What is the maximal possible size of a permutation code $\mathcal{C}$ with $d = 5$? Derive an analogue of the sphere-packing (Hamming) bound for the permutation codes.

Solution:

(a) Take two codewords $\bar{\boldsymbol{x}} = (x_1, x_2, \cdots, x_n)$ and $\bar{\boldsymbol{y}} = (y_1, y_2, \cdots, y_n)$ in $\mathcal{C}$, $\bar{\boldsymbol{x}} \neq \bar{\boldsymbol{y}}$. Then, there exists a coordinate $i \in \{1, 2, \cdots, n\}$, such that $x_i \neq y_i$.

Observe that each symbol $\{0, 1, 2, \cdots, n-1\}$ appears exactly once in $\bar{\boldsymbol{x}}$ and in $\bar{\boldsymbol{y}}$.

Let us ask the question: in what position in $\bar{\boldsymbol{x}}$ appears the symbol y_i? It appears in position different from i (because in position i we have x_i). Denote that position as j. Then, what symbol appears in position j in $\bar{\boldsymbol{y}}$? It is a symbol different from $x_j = y_i$. Therefore, $\bar{\boldsymbol{x}}$ and $\bar{\boldsymbol{y}}$ differ in at least two positions, i and j, so $\mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) \geq 2$.

(b) The codewords of $\mathcal{C}$ are permutations of elements $\{0, 1, 2, \cdots, n-1\}$. The number of permutations is $n!$. Therefore, the maximal size is $n!$.

Note: observe that due to (a), any two codewords are at distance 2 at least. Therefore, the set of all $n!$ permutations, as a code, has minimum distance at least 2. Therefore, $n!$ is indeed achievable.

(c) Let $\bar{\boldsymbol{x}} \in \mathcal{C}$. The number of codewords at distance 0 from $\bar{\boldsymbol{x}}$ is 1, it is $\bar{\boldsymbol{x}}$ itself. Due to (a), there are no codewords at distance 1 from $\bar{\boldsymbol{x}}$.

Finally, assume that $\bar{\boldsymbol{y}} \in \mathcal{C}$ and $\mathsf{d}_H(\bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}) = 2$. There are two positions where $\bar{\boldsymbol{x}}$ and $\bar{\boldsymbol{y}}$ differ, say, i and j. Then, $x_i = y_j$ and $x_j = y_i$. Therefore, $\bar{\boldsymbol{y}}$ is obtained from $\bar{\boldsymbol{x}}$ by choosing two positions i and j, and then by exchanging entries in those positions. The number of ways to choose positions i and j is $\binom{n}{2}$, and each choice gives a different codeword at distance 2.

In summary, the maximal number of codewords at distance at most $r = 2$ is:

$$1 + \binom{n}{2} .$$

This is a volume of an analogue of a sphere of radius 2.

(d) Consider the universe of all permutation vectors of length n over $\{0, 1, 2, \cdots, n-1\}$. There are $n!$ such vectors.

As computed in (c), the volume of the sphere of radius 2 is

$$1 + \binom{n}{2} .$$

Since $d = 5$, due to triangle inequality for the Hamming distance, the spheres of radius 2 around the codewords are disjoint. Therefore,

$$M \leq \frac{n!}{1 + \binom{n}{2}} .$$

Alternative solution to (d)

(This solution is correct in principle, but it is not the one that we had in mind.)

Permutation code can be viewed as a regular code. Then, the universe of all vectors of length n over $\mathbb{F}$ has size n^n. The volume of the sphere of radius 2 around any codeword is

$$\sum_{i=0}^{2} \binom{n}{i} (n-1)^i = 1 + n \cdot (n-1) + \binom{n}{2} \cdot (n-1)^2 .$$

Since $d = 5$, all spheres of radius 2 are disjoint. Therefore, by using the sphere-packing bound from the class, we obtain

$$M \leq \frac{n^n}{1 + n \cdot (n-1) + \binom{n}{2} \cdot (n-1)^2} .$$

Question 3 (40 points).

Let $\mathbb{F} = \mathbb{F}_2$ be a finite field with two elements and $\mathcal{C}$ be an $[n, k, d]$ code over $\mathbb{F}$, defined using the following generator matrix

$$\boldsymbol{G} = \left(\begin{array}{c|c} 0\,0\,\cdots\,0 & 1\,1\,\cdots\,1 \\ \hline \boldsymbol{G}_1 & \boldsymbol{G}_2 \end{array}\right),$$

where the number of 1's in the first row equals d. Let $\mathcal{C}_1$ be the linear $[n_1 = n - d, k_1, d_1]$ code over $\mathbb{F}$, which is spanned by the rows of $\boldsymbol{G}_1$, and $\mathcal{C}_2$ be the linear $[n_2 = d, k_2, d_2]$ code over $\mathbb{F}$, which is spanned by the rows of $\boldsymbol{G}_2$.

(a) Take

$$\boldsymbol{G}_1 = \boldsymbol{G}_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

What are the corresponding values of n, k and d?

Solution

We have:

$$\boldsymbol{G} = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right)$$

n is a number of columns in $\boldsymbol{G}$, i.e. 6.

k is number of rows in $\boldsymbol{G}$, i.e. we just need to check that rank of such $\boldsymbol{G}$ is 3 indeed. But for that we can just consider the matrix formed by the last three columns of $\boldsymbol{G}$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

and they form a full-rank matrix indeed.

Now let us find d. Since each row of a generator matrix is a codeword, and the first row of $\boldsymbol{G}$ has weight 3, then we know already that $d \leq 3$. Let us see if there are codewords of weight strictly less than 3.

Observe the following property of the code $\mathcal{C}$ – if the first three components of a codeword are (c_1, c_2, c_3) then the remaining three are either also (c_1, c_2, c_3) or $(c_1 + 1, c_2 + 1, c_3 + 1)$. This is because $\boldsymbol{G}_1 = \boldsymbol{G}_2$.

If weight of the first three components is $w_H((c_1, c_2, c_3)) = w$, then weight of the remaining three components is either w or $3 - w$. Hence in total the weight of the whole codeword is either $2w$ or $w + (3 - w) = 3$. We are interested in the former case with $w = 1$. However, (c_1, c_2, c_3) is spanned by linear combinations of $\boldsymbol{G}_1$ and, therefore, it has weight either 0 or 2 (there are only four codewords in the code defined by $\boldsymbol{G}_1$). This shows that $d = 3$.

Alternative way to show that $d = 3$ is simply by checking all seven non-zero codewords.

(b) (1) Show that if the rows of $\boldsymbol{G}_1$ are linearly dependent, then there exist two different non-zero codewords $\bar{\boldsymbol{b}}, \bar{\boldsymbol{c}} \in \mathcal{C}$, whose first n_1 coordinates are zeros (one of them is the first row of $\boldsymbol{G}$).

Solution

Since $\boldsymbol{G}_1$ has linearly dependent rows, there exists $\bar{\boldsymbol{x}} \neq \bar{\boldsymbol{0}}$, such that $\bar{\boldsymbol{x}} \cdot \boldsymbol{G}_1 = \bar{\boldsymbol{0}}$. Therefore codewords $(0 \mid \bar{\boldsymbol{x}}) \cdot \boldsymbol{G}$ and $(1 \mid \bar{\boldsymbol{x}}) \cdot \boldsymbol{G}$ both have zeroes in their first n_1 coordinates. They are different as they are obtained from different information messages $(0 \mid \bar{\boldsymbol{x}}) \neq (1 \mid \bar{\boldsymbol{x}})$.

(2) By using the result in (b-1), show that if the rows of $\boldsymbol{G}_1$ are linearly dependent, then there exists a codeword $\bar{\boldsymbol{b}} \in \mathcal{C}$ with weight strictly less than d. Observe a contradiction, and conclude that the rows of $\boldsymbol{G}_1$ must be linearly independent.

Solution

In (b-1) we showed that there exist $\bar{\boldsymbol{b}}$ and $\bar{\boldsymbol{c}}$ as above, $\bar{\boldsymbol{b}} \neq \bar{\boldsymbol{c}}$. On the other hand they both have zeroes in the first n_1 positions and, since the minimum distance of $\mathcal{C}$ is d, they should have all ones in the remaining $n - n_1 = d$ positions. Hence they are equal! This contradiction proves that the assumptions was wrong and rows of $\boldsymbol{G}_1$ cannot be linearly dependent.

(c) (1) Show that if $(\bar{\boldsymbol{c}}_1 | \bar{\boldsymbol{c}}_2) \in \mathcal{C}$, where $\bar{\boldsymbol{c}}_1 \in \mathcal{C}_1$, then either $\bar{\boldsymbol{c}}_2 \in \mathcal{C}_2$ or $\bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}} \in \mathcal{C}_2$, where $\bar{\boldsymbol{e}} = (1\,1 \cdots 1)$. Conclude that if $\bar{\boldsymbol{c}}_1$ has weight exactly d_1, then both $\bar{\boldsymbol{c}}_2$ and $\bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}}$ have weight at least $d - d_1$.

Solution

Each codeword in $\mathcal{C}$ can be represented uniquely as $(x_1, x_2, \cdots, x_k) \cdot \boldsymbol{G}$. With this representation, $\bar{\boldsymbol{c}}_1 = (x_2, \cdots, x_k) \cdot \boldsymbol{G}_1$ and $\bar{\boldsymbol{c}}_2 = (x_2, \cdots, x_k) \cdot \boldsymbol{G}_2 + (x_1, x_1, \cdots, x_1)$. If $x_1 = 0$, we have $\bar{\boldsymbol{c}}_2 = (x_2, \cdots, x_k) \cdot \boldsymbol{G}_2 \in \mathcal{C}_2$. And if $x_2 = 1$ we have $\bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}} = (x_2, \cdots, x_k) \cdot \boldsymbol{G}_2 \in \mathcal{C}_2$.

Also, since $(\bar{\boldsymbol{c}}_1 | \bar{\boldsymbol{c}}_2) \in \mathcal{C}$, we have $d \leq w_H\left((\bar{\boldsymbol{c}}_1 | \bar{\boldsymbol{c}}_2)\right) = w_H(\bar{\boldsymbol{c}}_1) + w_H(\bar{\boldsymbol{c}}_2) = d_1 + w_H(\bar{\boldsymbol{c}}_2)$ and, hence, $w_H(\bar{\boldsymbol{c}}_2) \geq d - d_1$.

Next, $(\bar{\boldsymbol{c}}_1 | \bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}})$ can be obtained as the sum of $(\bar{\boldsymbol{c}}_1 | \bar{\boldsymbol{c}}_2)$ and the first row of $\boldsymbol{G}$ (because of linearity of the code). Then, it also holds $d \leq w_H((\bar{\boldsymbol{c}}_1 | \bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}})) = d_1 + w_H(\bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}})$ and we automatically get what we need.

(2) Show that $d_1 \geq d_2$.

Solution

It must hold that $d_2 \leq n_2 = d$. If $d_1 \geq d$, then $d_1 \geq d_2$.

Now, assume that $d_1 < d$. Take a word $(\bar{\boldsymbol{c}}_1 | \bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}}) \in \mathcal{C}$, such that $w_H(\bar{\boldsymbol{c}}_1) = d_1$. Let $w_H(\bar{\boldsymbol{c}}_2) = \xi_2$. Then $\xi_2 \geq d_2$ or $\xi_2 = 0$. The case $\xi_2 = 0$ is not possible due to (c-1). We have that $w_H(\bar{\boldsymbol{c}}_2 + \bar{\boldsymbol{e}}) = d - \xi_2 \leq d - d_2$.

Now, $(\bar{\boldsymbol{c}}_1|\bar{\boldsymbol{c}}_2+\bar{\boldsymbol{e}})$ is a non-zero codeword of $\mathcal{C}$ and therefore it has weight at least d.

$$d \leq w_H(\bar{\boldsymbol{c}}_1|\bar{\boldsymbol{c}}_2+\bar{\boldsymbol{e}}) = w_H(\bar{\boldsymbol{c}}_1) + w_H(\bar{\boldsymbol{c}}_2+\bar{\boldsymbol{e}}) = d_1 + (d-\xi_2) \leq d_1 + d - d_2 \ .$$

By comparing the right-most and the left-most expressions, $d_1 \geq d_2$.

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

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

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

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

(a) Find the syndrome polynomial $S(x)$.

Solution

First, we convert elements of the parity-check matrix $\boldsymbol{H}$ to integers from 0 to 6:

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

Then syndrome vector is

$$\bar{\boldsymbol{s}}^T = \boldsymbol{H} \cdot \bar{\boldsymbol{y}}^T = (5, 2, 0, 1)^T.$$

From this we obtain the syndrome polynomial: $S(x) = x^3 + 2x + 5$.

(b) Find the error-locator and the error-evaluator polynomials by either Peterson-Gorenstein-Zierler method or by Euclid's algorithm.

Solution

We use extended Euclid's algorithm. Initialising polynomials:

$$r_{-1}(x) = a(x) = x^{d-1} = x^4, \quad r_0(x) = b(x) = S(x) = x^3 + 2x + 5,$$
$$t_{-1}(x) = 0, \quad t_0(x) = 1.$$

Iteration 1.

$$r_{-1}(x) = q_1(x) r_0(x) + r_1(x)$$
$$x^4 = x(x^3 + 2x + 5) + (5x^2 + 2x)$$

Hence $q_1(x) = x$ and $r_1(x) = 5x^2 + 2x$.

$$t_{-1}(x) = q_1(x)t_0(x) + t_1(x)$$
$$0 = x \cdot 1 + 6x$$

Thus $t_1(x) = 6x$. Further, $\deg r_1(x) = 2 \not< \frac{d-1}{2} = 2$ and we continue.
Iteration 2.

$$r_0(x) = q_2(x)r_1(x) + r_2(x)$$
$$x^3 + 2x + 5 = (3x + 3) \cdot (5x^2 + 2x) + (3x + 5)$$

Hence $q_2(x) = 3x + 3$ and $r_2(x) = 3x + 5$.

$$t_0(x) = q_2(x)t_1(x) + t_2(x)$$
$$1 = (3x + 3) \cdot 6x + (3x^2 + 3x + 1)$$

Thus $t_2(x) = 3x^2 + 3x + 1$. Now $\deg r_2(x) = 1 < \frac{d-1}{2} = 2$ and we stop.
Since $t_2(0) = 1$, we can already obtain:

$$\Lambda(x) = t_2(x) = 3x^2 + 3x + 1 \text{ and } \Gamma(x) = r_2(x) = 3x + 5\,.$$

(c) What are the error locations and error values?

Solution

We employ Forney's algorithm. For that we note that $\Lambda'(x) = 6x + 3$.

j	1	2	3	4	5	6
α_j	1	2	3	4	5	6
α_j^{-1}	1	4	5	2	3	6
$\Lambda(\alpha_j^{-1})$	0	5	0	5	2	1
e_j	3	0	2	0	0	0

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

Solution

$$\bar{\boldsymbol{c}} = \bar{\boldsymbol{y}} - \bar{\boldsymbol{e}} = (0, 1, 3, 6, 3, 1)\,.$$

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

Solution

$$\boldsymbol{H} \cdot \bar{\boldsymbol{c}}^T = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \\ 6 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 14 \\ 56 \\ 35 \\ 49 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

and $\bar{\boldsymbol{c}}$ is indeed a codeword.