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

Final exam: solutions

Instructors: Vitaly Skachek, Yauhen Yakimenka January 24th, 2018

Student name: _____

Student ID: _____

1. This exam contains 9 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).

A code $\mathcal{C}$ is defined as the following set of vectors over $\mathbb{F}_3 = \{0, 1, 2\}$:

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

where

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

(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)
- Trivially, the length $n = 6$.
- The first three rows are linearly dependent (the third row is obtained as the first row added to 2 × second row). Therefore, the rank of $\boldsymbol{H}$ is at most 3. It is exactly 3 because the first three columns, rows 1, 2 and 4, contain a 3×3 diagonal matrix

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

  Thus, $n - k = 3$, $k = 3$.
- Finally, $(\,0\,0\,0\,0\,1\,0\,)$ is a codeword, so the minimum distance $d = 1$.

(b) Since $k = 3$, it is enough to show any 3 linearly independent codewords. One can pick, for example the rows of the following matrix

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} .$$

□

Question 2 (30 points).

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be linear codes of the same length n over the finite field $\mathbb{F}_3 = \{0, 1, 2\}$, such that $\mathcal{C}_1 \cap \mathcal{C}_2 = \{\bar{\mathbf{0}}\}$. Let $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ be parity-check matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Define the code

$$\mathcal{C}_3 = \{ \, (\, \bar{\boldsymbol{x}} + \bar{\boldsymbol{y}} \mid \bar{\boldsymbol{x}} + 2 \cdot \bar{\boldsymbol{y}} \,) \; : \; \bar{\boldsymbol{x}} \in \mathcal{C}_1 \text{ and } \bar{\boldsymbol{y}} \in \mathcal{C}_2 \}$$

of length n. For $i = 1, 2, 3$, let $k_i \geq 1$ be the dimension of $\mathcal{C}_i$ and d_i be its minimum distance.

(a) Show that the code $\mathcal{C}_3$ is linear.

(b) Show that $k_3 = k_1 + k_2$.

(c) Show that

$$\boldsymbol{H}_3 = \left(\begin{array}{c|c} \boldsymbol{H}_1 & \boldsymbol{H}_1 \\ \hline -\boldsymbol{H}_2 & \boldsymbol{H}_2 \end{array} \right)$$

is a parity-check matrix of $\mathcal{C}_3$.

(d) Is it true that $d_3 \geq \max\{d_1, d_2\}$? If yes – prove, otherwise – disprove or show a counterexample.

Solution. For convenience, we will use the fact that over field $\mathbb{F}_3$, $\bar{\boldsymbol{x}} + 2\bar{\boldsymbol{y}} = \bar{\boldsymbol{x}} - \bar{\boldsymbol{y}}$.

(a) The code $\mathcal{C}_3$ is linear if and only if for all $\alpha \in \mathbb{F}_3$, $\bar{\boldsymbol{x}}_1, \bar{\boldsymbol{x}}_2 \in \mathcal{C}_1$, $\bar{\boldsymbol{y}}_1, \bar{\boldsymbol{y}}_2 \in \mathcal{C}_2$, it holds that

$$\alpha \left((\bar{\boldsymbol{x}}_1 + \bar{\boldsymbol{y}}_1 \mid \bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{y}}_1) + (\bar{\boldsymbol{x}}_2 + \bar{\boldsymbol{y}}_2 \mid \bar{\boldsymbol{x}}_2 - \bar{\boldsymbol{y}}_2) \right) = \alpha(\bar{\boldsymbol{x}}_1 + \bar{\boldsymbol{y}}_1 \mid \bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{y}}_1) + \alpha(\bar{\boldsymbol{x}}_2 + \bar{\boldsymbol{y}}_2 \mid \bar{\boldsymbol{x}}_2 - \bar{\boldsymbol{y}}_2) \, ,$$

which follows immediately from linearity of vector operations (addition and multiplication by a scalar).

(b) In the definition of $\mathcal{C}_3$, we have $|\mathcal{C}_1|$ choices for $\bar{\boldsymbol{x}}$ and $|\mathcal{C}_2|$ choices for $\bar{\boldsymbol{y}}$. Let us show that different pairs $(\bar{\boldsymbol{x}}_1, \bar{\boldsymbol{y}}_1)$ and $(\bar{\boldsymbol{x}}_2, \bar{\boldsymbol{y}}_2)$ produce different vectors of $\mathcal{C}_3$. Assume to the contrary that $(\bar{\boldsymbol{x}}_1 + \bar{\boldsymbol{y}}_1 \mid \bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{y}}_1) = (\bar{\boldsymbol{x}}_2 + \bar{\boldsymbol{y}}_2 \mid \bar{\boldsymbol{x}}_2 - \bar{\boldsymbol{y}}_2)$ or, equivalently, that $(\bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{x}}_2 + \bar{\boldsymbol{y}}_1 - \bar{\boldsymbol{y}}_2 \mid \bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{x}}_2 - \bar{\boldsymbol{y}}_1 + \bar{\boldsymbol{y}}_2) = \bar{0}$. This can be written as follows:

$$\begin{cases} \bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{x}}_2 + \bar{\boldsymbol{y}}_1 - \bar{\boldsymbol{y}}_2 = \bar{0} \, , \\ \bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{x}}_2 - \bar{\boldsymbol{y}}_1 + \bar{\boldsymbol{y}}_2 = \bar{0} \, . \end{cases}$$

Summing up the equations, we obtain $2(\bar{\boldsymbol{x}}_1 - \bar{\boldsymbol{x}}_2) = \bar{0}$ which means that $\bar{\boldsymbol{x}}_1 = \bar{\boldsymbol{x}}_2$.

Subtracting the equations, we obtain $2(\bar{\boldsymbol{y}}_1 - \bar{\boldsymbol{y}}_2) = \bar{0}$ and $\bar{\boldsymbol{y}}_1 = \bar{\boldsymbol{y}}_2$.

Therefore, different pairs $(\bar{\boldsymbol{x}}_1, \bar{\boldsymbol{y}}_1)$ and $(\bar{\boldsymbol{x}}_2, \bar{\boldsymbol{y}}_2)$ produce different vectors of $\mathcal{C}_3$ indeed. Because of that, due to rule of product in combinatorics, $3^{k_3} = |\mathcal{C}_3| = |\mathcal{C}_2| \cdot |\mathcal{C}_1| = 3^{k_2 + k_1}$, and we have proven the required statement.

(c) To show that $\boldsymbol{H}_3$ is a parity-check matrix of $\mathcal{C}_3$ we need to prove that $\boldsymbol{H}_3 \cdot \bar{\boldsymbol{c}}^T = \bar{0}$ is satisfied for all the codewords from $\mathcal{C}_3$, and only for them.

Take any $(\bar{\boldsymbol{x}} + \bar{\boldsymbol{y}} \,|\, \bar{\boldsymbol{x}} - \bar{\boldsymbol{y}}) \in \mathcal{C}_3$ (with $\bar{\boldsymbol{x}} \in \mathcal{C}_1$ and $\bar{\boldsymbol{y}} \in \mathcal{C}_2$). Then

$$\left(\begin{array}{c|c} \boldsymbol{H}_1 & \boldsymbol{H}_1 \\ \hline -\boldsymbol{H}_2 & \boldsymbol{H}_2 \end{array}\right) \cdot \bar{\boldsymbol{c}}^T = \left(\begin{array}{c} \boldsymbol{H}_1 \cdot (\bar{\boldsymbol{x}}^T + \bar{\boldsymbol{y}}^T) + \boldsymbol{H}_1 \cdot (\bar{\boldsymbol{x}}^T - \bar{\boldsymbol{y}}^T) \\ \hline -\boldsymbol{H}_2 \cdot (\bar{\boldsymbol{x}}^T + \bar{\boldsymbol{y}}^T) + \boldsymbol{H}_2 \cdot (\bar{\boldsymbol{x}}^T - \bar{\boldsymbol{y}}^T) \end{array}\right) = \left(\begin{array}{c} 2\boldsymbol{H}_1 \cdot \bar{\boldsymbol{x}}^T \\ \hline -2\boldsymbol{H}_2 \cdot \bar{\boldsymbol{y}}^T \end{array}\right) = \binom{\bar{0}}{\bar{0}} = \bar{0}\,,$$

since $\bar{\boldsymbol{x}} \in \mathcal{C}_1$ and $\bar{\boldsymbol{y}} \in \mathcal{C}_2$.

In the opposite direction, take any vector[1] $(\bar{\boldsymbol{v}} \,|\, \bar{\boldsymbol{w}})$, such that $\boldsymbol{H}_3 \cdot (\bar{\boldsymbol{v}} \,|\, \bar{\boldsymbol{w}})^T = \bar{0}$. Then we can write:

$$\bar{0} = \left(\begin{array}{c|c} \boldsymbol{H}_1 & \boldsymbol{H}_1 \\ \hline -\boldsymbol{H}_2 & \boldsymbol{H}_2 \end{array}\right) \cdot (\bar{\boldsymbol{v}} \,|\, \bar{\boldsymbol{w}})^T = \left(\begin{array}{c} \boldsymbol{H}_1 \cdot (\bar{\boldsymbol{v}}^T + \bar{\boldsymbol{w}}^T) \\ \hline -\boldsymbol{H}_2 \cdot (\bar{\boldsymbol{v}}^T - \bar{\boldsymbol{w}}^T) \end{array}\right).$$

This means that $\bar{\boldsymbol{x}}' = \bar{\boldsymbol{v}} + \bar{\boldsymbol{w}} \in \mathcal{C}_1$ and $\bar{\boldsymbol{y}}' = \bar{\boldsymbol{v}} - \bar{\boldsymbol{w}} \in \mathcal{C}_2$. But then $(\bar{\boldsymbol{v}}|\bar{\boldsymbol{w}}) = (\bar{\boldsymbol{x}}' + \bar{\boldsymbol{y}}' | \bar{\boldsymbol{x}}' - \bar{\boldsymbol{y}}') \in \mathcal{C}_3$ by definition of $\mathcal{C}_3$.

(d) The statement is not true and the counter-example can be as follows. Take $[6, 1, 6]$ code $\mathcal{C}_1 = \{000000, 111111, 222222\}$ and $[6, 1, 2]$ code $\mathcal{C}_2 = \{000000, 001001, 002002\}$. Then the code $\mathcal{C}_3$ contains the codeword $(000000 + 001001|000000 - 001001) = (001001|002002)$ of weight 4 and thus $d_3 \leq 4$. But $\max\{d_1, d_2\} = 6$.

Note. One of the correct statements can be for instance the following: $d_3 \geq \min\{d_1, d_2\}$.

□

[1] Splitting into $\bar{\boldsymbol{v}}$ and $\bar{\boldsymbol{w}}$ is half-half.

Question 3 (30 points).

Let $\mathcal{C}$ be an MDS $[n, k, d]$ code over the finite field $\mathbb{F}$. Denote by

$$\boldsymbol{H} = \begin{pmatrix} h_{1,1} & h_{1,2} & h_{1,3} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & h_{2,3} & \cdots & h_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1} & h_{n-k,2} & h_{n-k,3} & \cdots & h_{n-k,n} \end{pmatrix}$$

an $(n-k) \times n$ parity-check matrix of $\mathcal{C}$.

(a) Let $\boldsymbol{H}_1$ be a parity-check matrix that is obtained by adding an *arbitrary column* (of length $n-k$) to $\boldsymbol{H}$. Is it always true that $\boldsymbol{H}_1$ is a parity-check matrix of an $[n+1, k+1, d]$ MDS code over $\mathbb{F}$? If yes – prove, otherwise show a counterexample or explain.

(b) Show that there exists a parity-check matrix $\boldsymbol{H}'$ of $\mathcal{C}$ of the following form:

$$\boldsymbol{H}' = (\, \boldsymbol{I} \mid \boldsymbol{A} \,) \ ,$$

where $\boldsymbol{I}$ is the $(n-k) \times (n-k)$ identity matrix, and $\boldsymbol{A}$ is an $(n-k) \times k$ matrix, both over $\mathbb{F}$.

(c) Let $\boldsymbol{H}_2$ be a matrix obtained from $\boldsymbol{H}$ by replacing one of its entries $h_{i,j}$ by zero. Is it always true that $\boldsymbol{H}_2$ is a parity-check matrix of an MDS code over $\mathbb{F}$ with minimum distance $\geq d-1$? If yes – prove, otherwise show a counterexample or explain.

(d) Let $\boldsymbol{H}_3$ be a parity-check matrix that is obtained by removing any t columns from $\boldsymbol{H}$, $t < d$. Is it always true that $\boldsymbol{H}_3$ is a parity-check matrix of an MDS code over $\mathbb{F}$? If yes – prove, otherwise show a counterexample or explain.

(e) Let $\boldsymbol{H}_4$ be a parity-check matrix that is obtained by removing any t rows from $\boldsymbol{H}$, $t < n-k$. Is it always true that $\boldsymbol{H}_4$ is a parity-check matrix of an MDS code over $\mathbb{F}$? If yes – prove, otherwise show a counterexample or explain.

Solution.

(a) **False.** Assume that $d \geq 3$ (there are many such MDS codes). Let us append the first column of $\boldsymbol{H}$ as the last column to $\boldsymbol{H}$. The resulting code has minimum distance ≤ 2 since $(\, 1\, 0\, 0 \cdots 0\, 1 \,)$ is a codeword.

(b) Take a parity-check matrix $\boldsymbol{H}$ of an MDS code $\mathcal{C}$ of the following form:

$$\boldsymbol{H} = (\, \boldsymbol{B} \mid \boldsymbol{A} \,) \ ,$$

where $\boldsymbol{B}$ is the $(n-k) \times (n-k)$ matrix, and $\boldsymbol{A}$ is an $(n-k) \times k$ matrix, both over $\mathbb{F}$. The code $\mathcal{C}$ is defined as

$$\mathcal{C} = \{ \boldsymbol{x} \in \mathbb{F}^n \ : \ \boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{0}^T \} \ .$$

All $n-k$ columns of $\boldsymbol{B}$ are linearly independent. This was shown in the class (otherwise, there is a nonzero codeword of weight $\leq n-k=d-1$, which is not possible.) Therefore, $\boldsymbol{B}$ is invertible. Denote its inverse $\boldsymbol{B}^{-1}$. Take

$$\boldsymbol{H}' \triangleq \boldsymbol{B}^{-1}\boldsymbol{H} = \boldsymbol{B}^{-1} \cdot (\, \boldsymbol{B} \mid \boldsymbol{A} \,) = \left(\boldsymbol{I} \mid \boldsymbol{A}' \right) .$$

We observe:

- For any codeword $\boldsymbol{c} \in \mathcal{C}$,

$$\boldsymbol{H}'\boldsymbol{c}^T = \boldsymbol{B}^{-1}\boldsymbol{H}\boldsymbol{c}^T = \boldsymbol{B}^{-1}\boldsymbol{0}^T = \boldsymbol{0}^T .$$

- For any non-codeword $\boldsymbol{x} \notin \mathcal{C}$,

$$\boldsymbol{H}\boldsymbol{x}^T \neq \boldsymbol{0}^T .$$

  Then, if by contrary $\boldsymbol{H}'\boldsymbol{x}^T = \boldsymbol{0}^T$, we obtain

$$\boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{B}\boldsymbol{B}^{-1}\boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{B}\boldsymbol{H}'\boldsymbol{x}^T = \boldsymbol{0}^T ,$$

  which is a contradiction.

We conclude that $\boldsymbol{H}'\boldsymbol{x}^T = \boldsymbol{0}^T$ if and only if $\boldsymbol{x} \in \mathcal{C}$, and so $\boldsymbol{H}'$ is a parity-check matrix of $\mathcal{C}$ of the required form.

(c) **False.** Take $\mathcal{C}$ to be an MDS code with $d \geq 3$. From (b), there exists a parity-check matrix of $\mathcal{C}$ in the form

$$\boldsymbol{H} = (\, \boldsymbol{I} \mid \boldsymbol{A} \,) .$$

Replace the entry '1' in the first column and first row to '0'. The resulting matrix $\boldsymbol{H}_2$ has in its first column all zeros. Therefore, the resulting code has minimum distance $d = 1$.

(d) **True.** Similarly to (b), we use the fact that the code is MDS if and only if any $(n-k)\times(n-k)$ sub-matrix of $\boldsymbol{H}$ is a full rank (this was shown in the class. A quick way to see that – if $(n-k)\times(n-k)$ sub-matrix of $\boldsymbol{H}$ is not a full rank, then there exists a nonzero codeword of weight at most $d-1$).

If we remove some columns of $\boldsymbol{H}$, in $\boldsymbol{H}_3$ any $(n-k)\times(n-k)$ sub-matrix is still a full rank. Therefore, the resulting code is MDS.

(e) **False.** Similar to (c). Take $\mathcal{C}$ to be an MDS code with $n-k=d-1 \geq 3$. From (b), there exists a parity-check matrix of $\mathcal{C}$ in the form

$$\boldsymbol{H} = (\, \boldsymbol{I} \mid \boldsymbol{A} \,) .$$

Remove $t = 1$ first row of $\boldsymbol{H}$. The resulting matrix $\boldsymbol{H}_4$ has in its first column all zeros. Therefore, the resulting code has minimum distance 1.

Denote new code parameters as n', k' and d'. The length of the new code is $n' = n$, the dimension is $k' \leq k+1$ (we removed only one row in the parity-check matrix). We have

$$n' - k' \geq n - (k+1) = d - 2 \geq 2 \neq d' - 1 = 0 .$$

Therefore, the new code is not 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 of the code given by

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

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 $v_2 = v_4 = v_6 = 4$.

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

Solution.

(a) To find syndrom polynomial, we multiply the parity-check matrix $\boldsymbol{H}$ by received word $\bar{\boldsymbol{y}}$:

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

Therefore the syndrom is $S(x) = 3x^3 + 2x^2 + x + 5$.

(b) The linear system for Peterson-Gorenstein-Zieter algorithm:

$$\left(\begin{array}{ccc} 5 & 0 & 0 \\ 1 & 5 & 0 \\ \hline 2 & 1 & 5 \\ 3 & 2 & 1 \end{array}\right) \cdot \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \end{pmatrix} = \left(\begin{array}{c} \gamma_0 \\ \gamma_1 \\ \hline 0 \\ 0 \end{array}\right)$$

From the lower part, setting for example $\lambda_0 = 1$, we obtain:

$$\begin{cases} \lambda_0 = 1\,, \\ 2 + \lambda_1 + 5\lambda_2 = 0\,, \\ 3 + 2\lambda_1 + \lambda_2 = 0\,, \end{cases} \iff \begin{cases} \lambda_0 = 1\,, \\ \lambda_1 = 4\,, \\ \lambda_2 = 3\,. \end{cases}$$

Then from the upper part, $\gamma_0 = 5\lambda_0 = 5$ and $\gamma_1 = \lambda_0 + 5\lambda_1 = 0$, and we get polynomials[2] $\Lambda(x) = 3x^2 + 4x + 1$ and $\Gamma(x) = 5$.

Alternatively, we can find the same polynomials from the Euclid's algorithm. The steps are as follows.

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

Iteration $i = 1$.

$$r_{-1}(x) = \underline{q_1(x)} \cdot r_0(x) + \underline{r_1(x)} \textbf{ gives } x^4 = (\underline{5x+6}) \cdot (3x^3 + 2x^2 + x + 5) + \underline{4x^2 + 4x + 5}$$
$$t_{-1}(x) = q_1(x) \cdot t_0(x) + \underline{t_1(x)} \textbf{ gives } 0 = (5x+6) \cdot 1 + \underline{2x+1}$$

$\deg r_1(x) = 2 \not< \frac{d-1}{2} = 2$, thus, we continue.

Iteration $i = 2$.

$$r_0(x) = \underline{q_2(x)} \cdot r_1(x) + \underline{r_2(x)} \textbf{ gives } 3x^3 + 2x^2 + x + 5 = (\underline{6x+5}) * (4x^2 + 4x + 5) + \underline{1}$$
$$t_0(x) = q_2(x) \cdot t_1(x) + \underline{t_2(x)} \textbf{ gives } 1 = (6x+5) * (2x+1) + \underline{2x^2 + 5x + 3}$$

$\deg r_2(x) = 0 < \frac{d-1}{2} = 2$, and we stop. Assign $\Lambda(x) = t_2(x) = 2x^2 + 5x + 3$ and $\Gamma(x) = r_2(x) = 1$.

Since $c = \Lambda(0) = 3 \neq 0$, we re-assign $\Lambda(x) = (2x^2 + 5x + 3) \cdot 3^{-1} = 3x^2 + 4x + 1$ and $\Gamma(x) = 1 \cdot 3^{-1} = 5$.

(c)

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

[2]Note that $\Lambda(0) = 1$ already.

(d) Then $\bar{\boldsymbol{c}} = \bar{\boldsymbol{y}} - \bar{\boldsymbol{e}} = (1, 5, 1, 0, 3, 6)$.

(e) Checking that we obtained the correct result:

$$\boldsymbol{H} \cdot \bar{\boldsymbol{c}}^T = \begin{pmatrix} 1 & 4 & 1 & 4 & 1 & 4 \\ 1 & 1 & 3 & 2 & 5 & 3 \\ 1 & 2 & 2 & 1 & 4 & 4 \\ 1 & 4 & 6 & 4 & 6 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \\ 1 \\ 0 \\ 3 \\ 6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} .$$

□