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

Final exam

Instructors: Vitaly Skachek, Eldho K. Thomas January 3rd, 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 3×4 parity-check matrices:

$$\mathcal{H}_1 = \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{pmatrix} \qquad \text{and} \qquad \mathcal{H}_2 = \begin{pmatrix} 1 & 3 & 0 & 3 \\ 0 & 1 & 3 & 0 \\ 1 & 0 & 1 & 3 \end{pmatrix},$$

that correspond to the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, 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.

Solution:

(a) The matrix $\mathcal{H}_1$ has a row-echelon form, its rows are linearly independent, and therefore its rank is 3. The dimension of $\mathcal{C}_1$ is $n - \text{rank}(\mathcal{H}_1) = 4 - 3 = 1$. By contrast, the rows of matrix $\mathcal{H}_2$ are linearly dependent: the first row plus two times the second row gives the third row. Therefore, $\text{rank}(\mathcal{H}_2) \leq 2$, and so the dimension of $\mathcal{C}_2$ is at least 2. Thus, the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are different.

(b)
- It is straightforward to see that the length of each of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ is 4.
- As it is observed in (a), the dimension of $\mathcal{C}_1$ is 1. Also, it is observed in (a) that $\text{rank}(\mathcal{H}_2) \leq 2$. Additionally, the first two rows of $\mathcal{H}_2$ are linearly independent. Therefore, $\text{rank}(\mathcal{H}_2) = 2$, and so the dimension of $\mathcal{C}_2$ is exactly $n - \text{rank}(\mathcal{H}_2) = 4 - 2 = 2$.
- It was proved in the lecture that d is the minimum distance of a code, if it is the largest integer such that any $d - 1$ columns in a parity-check matrix of that code are linearly independent.
  For the code $\mathcal{C}_1$, every three columns are linearly independent. Indeed, columns $\{1, 2, 3\}$ are linearly independent due to a row-echelon form. Columns $\{1, 2, 4\}$ are also linearly independent due to a row-echelon form. It can be checked that the columns $\{1, 3, 4\}$ are linearly independent. Finally, the columns $\{2, 3, 4\}$ are also linearly independent (this can be shown by solving a system of 3 equations with 3 unknowns, or by computing the determinant). Conclusion: the minimum distance of $\mathcal{C}_1$ is 4.
  For the code $\mathcal{C}_2$, the first and the fourth columns are linearly dependent. On the other hand, every column alone is an independent set. Therefore, the minimum distance of $\mathcal{C}_2$ is 2.

Question 2 (30 points).

Definition: Let $\boldsymbol{A}$ be an $k_A \times n_A$ matrix over the finite field $\mathbb{F}$ given by:

$$\boldsymbol{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n_A} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n_A} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k_A,1} & a_{k_A,2} & a_{k_A,3} & \cdots & a_{k_A,n_A} \end{pmatrix} .$$

Let $\boldsymbol{B}$ be an $k_B \times n_B$ matrix over $\mathbb{F}$. Then, *the Kronecker product* $\boldsymbol{A} \otimes \boldsymbol{B}$ is the $k_A k_B \times n_A n_B$ block matrix:

$$\boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{1,1} \cdot \boldsymbol{B} & a_{1,2} \cdot \boldsymbol{B} & a_{1,3} \cdot \boldsymbol{B} & \cdots & a_{1,n_A} \cdot \boldsymbol{B} \\ a_{2,1} \cdot \boldsymbol{B} & a_{2,2} \cdot \boldsymbol{B} & a_{2,3} \cdot \boldsymbol{B} & \cdots & a_{2,n_A} \cdot \boldsymbol{B} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k_A,1} \cdot \boldsymbol{B} & a_{k_A,2} \cdot \boldsymbol{B} & a_{k_A,3} \cdot \boldsymbol{B} & \cdots & a_{k_A,n_A} \cdot \boldsymbol{B} \end{pmatrix} ,$$

where $a_{i,j} \cdot \boldsymbol{B}$ is a standard scalar-matrix multiplication.

Example: Take two matrices over $\mathbb{F}_3 = \{0, 1, 2\}$:

$$\boldsymbol{A} = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} \qquad \text{and} \qquad \boldsymbol{B} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} .$$

Then,

$$\boldsymbol{A} \otimes \boldsymbol{B} = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{array}\right) .$$

Tasks: Let $\mathcal{C}_A$ and $\mathcal{C}_B$ be two linear codes over $\mathbb{F}$ with parameters $[n_A, k_A, d_A]$ and $[n_B, k_B, d_B]$, and with generator matrices $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively. Let $\boldsymbol{A} \otimes \boldsymbol{B}$ be a generator matrix of an $[n, k, d]$ code $\mathcal{C}$ (after possible removal of linearly-dependent rows).

(a) Prove that $k = k_A \cdot k_B$ (Hint: it can be convenient to choose $\boldsymbol{A}$ in a systematic form – why it is always possible?)

(b) Show that $d \leq d_A \cdot d_B$.

Solution:

(a) First, without loss of generality assume that $\boldsymbol{A}$ has a systematic form. If not – since it is full-rank by the definition of the generator matrix, we can always find k_A columns which are linearly independent, and reorder the columns such that these k_A columns are the left-most k_A columns. This operation does not change the code parameters. Then, we can apply elementary row operations to the rows of the matrix with permuted columns, such that the left-most $k_A \times k_A$ submatrix is an identity. Elementary row operations do not change the

rowspace, i.e. they do not change the code. We conclude that there exists a systematic generator matrix for $\mathcal{C}_A$, for simplicity we will call it $\boldsymbol{A}$.

Next, the matrix $\boldsymbol{A} \otimes \boldsymbol{B}$ has the following form:

$$\boldsymbol{A} \otimes \boldsymbol{B} = \left(\begin{array}{cccc|ccc} 1 \cdot \boldsymbol{B} & 0 \cdot \boldsymbol{B} & \cdots & 0 \cdot \boldsymbol{B} & a_{1,k_A+1} \cdot \boldsymbol{B} & \cdots & a_{1,n} \cdot \boldsymbol{B} \\ 0 \cdot \boldsymbol{B} & 1 \cdot \boldsymbol{B} & \cdots & 0 \cdot \boldsymbol{B} & a_{2,k_A+1} \cdot \boldsymbol{B} & \cdots & a_{2,n} \cdot \boldsymbol{B} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 \cdot \boldsymbol{B} & 0 \cdot \boldsymbol{B} & \cdots & 1 \cdot \boldsymbol{B} & a_{k_A,k_A+1} \cdot \boldsymbol{B} & \cdots & a_{k_A,n} \cdot \boldsymbol{B} \end{array} \right) ,$$

Every column consists of k_A blocks, each block has k_B coordinates. Therefore, $\boldsymbol{A} \otimes \boldsymbol{B}$ has $k_A \cdot k_B$ rows. In order to show that this is the dimension of the code, it suffices to show that all rows of $\boldsymbol{A} \otimes \boldsymbol{B}$ are linearly independent.

Write down

$$\sum_{i=1}^{k_A \cdot k_B} \lambda_i \boldsymbol{r}_i = 0 ,$$

where $\boldsymbol{r}_i$ is the i-th row of $\boldsymbol{A} \otimes \boldsymbol{B}$, and λ_i are coefficients from $\mathbb{F}$.

From the left-most set of blocks in $\boldsymbol{A} \otimes \boldsymbol{B}$, we have that

$$\sum_{i=1}^{k_B} \lambda_i \boldsymbol{r}_i = 0 ,$$

and thus due to linear independence of the rows in $\boldsymbol{B}$, $\lambda_i = 0$ for $i = 1, 2, \cdots, k_B$.

From the second left-most set of blocks in $\boldsymbol{A} \otimes \boldsymbol{B}$, we have that

$$\sum_{i=k_B+1}^{2k_B} \lambda_i \boldsymbol{r}_i = 0 ,$$

and thus due to linear independence of the rows in $\boldsymbol{B}$, $\lambda_i = 0$ for $i = k_B + 1, k_B + 2, \cdots, 2k_B$.

By repeating the same argument on all blocks of the systematic part of $\boldsymbol{A}$, we conclude that $\lambda_i = 0$ for $i = 1, 2, \cdots, k_A k_B$. This implies linear independence of all the rows in $\boldsymbol{A} \otimes \boldsymbol{B}$, as required.

(b) Denote by $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_{k_A}$ the rows of $\boldsymbol{A}$. Assume that $\boldsymbol{a}_{min} = \sum_{i=1}^{k_A} \alpha_i \cdot \boldsymbol{a}_i$ is the codeword in $\mathcal{C}_A$ of the (minimum nonzero) weight d_A. Similarly, denote by $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_{k_B}$ the rows of $\boldsymbol{B}$, and assume that $\boldsymbol{b}_{min} = \sum_{j=1}^{k_B} \beta_j \cdot \boldsymbol{b}_j$ is the codeword in $\mathcal{C}_B$ of weight d_B.

Consider the codeword $\boldsymbol{c}_0$ of $\mathcal{C}$ obtained as

$$\boldsymbol{c}_0 = \sum_{i=1,\ldots,k_A; j=1,\ldots,k_B} \alpha_i \beta_j \cdot \boldsymbol{r}_{(i-1) \cdot k_B + j} = \sum_{i=1,\ldots,k_A} \alpha_i \cdot \left(\sum_{j=1,\ldots,k_B} \beta_j \cdot \boldsymbol{r}_{(i-1) \cdot k_B + j} \right) .$$

The rows $\boldsymbol{r}_\ell$ consist of n_A blocks of length n_B, and so $\boldsymbol{c}_0$ consists of similar blocks. Consider block ℓ in $\boldsymbol{c}_0$, $1 \leq \ell \leq n_A$. By the definition of the Kronecker product, it is equal to:

$$\boldsymbol{c}_\ell = \sum_{i=1,\ldots,k_A} \alpha_i \cdot \left(\sum_{j=1,\ldots,k_B} \beta_j \cdot a_{i,\ell} \cdot \boldsymbol{b}_j \right) = \sum_{i=1,\ldots,k_A} \alpha_i \cdot a_{i,\ell} \cdot \left(\sum_{j=1,\ldots,k_B} \beta_j \cdot \boldsymbol{b}_j \right) ,$$

where $a_{i,\ell}$ denotes entry in row i and column ℓ of $\boldsymbol{A}$. We obtain:

$$\boldsymbol{c}_\ell = \sum_{i=1,\ldots,k_A} \alpha_i \cdot a_{i,\ell} \cdot \boldsymbol{b}_{min} \ .$$

Now, observe that $\sum_{i=1,\ldots,k_A} \alpha_i \cdot a_{i,\ell}$ is equal to the ℓ-th symbol in $\boldsymbol{a}_{min}$. If this symbol is zero, then the whole block $\boldsymbol{c}_\ell$ is a block of zeros. If this symbol is not zero, then the block $\boldsymbol{c}_\ell$ has weight d_B. We conclude that the total weight of $\boldsymbol{c}_0$ is $d_A \cdot d_B > 0$.

It follows that $d \leq d_A \cdot d_B$. $\square$

Question 3 (30 points).

1. Let $\boldsymbol{H}$ be the following $(n-k) \times n$ **parity-check** matrix of an $[n, k, d]$ Reed-Solomon code $\mathcal{C}$ over the finite field $\mathbb{F}$,

$$\boldsymbol{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \alpha_3^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix},$$

   where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all distinct nonzero elements in $\mathbb{F}$.

   Consider the code $\mathcal{C}'$, whose parity-check matrix is

$$\boldsymbol{H}' = \left(\begin{array}{ccccc|c} 1 & 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n & 0 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \alpha_3^{n-k-1} & \cdots & \alpha_n^{n-k-1} & 0 \end{array}\right)$$

   over $\mathbb{F}$. Prove that $\mathcal{C}'$ has parameters $[n+1, k+1, d]$. Explain why $\mathcal{C}'$ is MDS.

2. Consider the code $\mathcal{D}$, whose **generator** matrix over $\mathbb{F}$ is $\boldsymbol{H}'$ as above. What are the parameters of $\mathcal{D}$? Show that $\mathcal{D}$ is MDS.

Solution:

1. First, we prove that any $(n-k) \times (n-k)$ submatrix of $\boldsymbol{H}$ is full rank.

   - If the submatrix does not contain the last column $(1, 0, 0, \cdots, 0)^T$, then it is a Vandermonde matrix. In the lecture, we computed its determinant, and proved that it is not equal to zero if all α_i are non-zero and distinct.
   - If the $(n-k) \times (n-k)$ submatrix of $\boldsymbol{H}$ contains the column $(1, 0, 0, \cdots, 0)^T$ of $\boldsymbol{H}$, then its has the following form:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_{i_1} & \alpha_{i_2} & \cdots & \alpha_{i_{n-k-1}} & 0 \\ \alpha_{i_1}^2 & \alpha_{i_2}^2 & \cdots & \alpha_{i_{n-k-1}}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{i_1}^{n-k-1} & \alpha_{i_2}^{n-k-1} & \cdots & \alpha_{i_{n-k-1}}^{n-k-1} & 0 \end{pmatrix}.$$

The determinant of this matrix is equal to determinant:

$$\det \begin{pmatrix} \alpha_{i_1} & \alpha_{i_2} & \cdots & \alpha_{i_{n-k-1}} \\ \alpha_{i_1}^2 & \alpha_{i_2}^2 & \cdots & \alpha_{i_{n-k-1}}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_1}^{n-k-1} & \alpha_{i_2}^{n-k-1} & \cdots & \alpha_{i_{n-k-1}}^{n-k-1} \end{pmatrix}$$

$$= \alpha_{i_1} \cdot \alpha_{i_2} \cdots \alpha_{i_{n-k-1}} \cdot \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{i_1} & \alpha_{i_2} & \cdots & \alpha_{i_{n-k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_1}^{n-k-2} & \alpha_{i_2}^{n-k-2} & \cdots & \alpha_{i_{n-k-1}}^{n-k-2} \end{pmatrix}$$

The latter matrix under determinant is Vandermonde matrix, and thus its determinant is non-zero. We obtain that the determinant of the product is non-zero as well.

Next, the length of $\mathcal{C}'$ is obviously $n+1$. Since all rows of $\boldsymbol{H}'$ are linearly independent, the dimension of $\mathcal{C}'$ is $(n+1)-(n-k)=k+1$. The minimum distance of the code is d if and only if d is the largest integer such that any $d-1$ columns are linearly independent. Thus, the minimum distance of $\mathcal{C}'$ is $d=n-k+1$.

We have that $n+1=(k+1)+(n-k+1)-1$, and thus the code $\mathcal{C}'$ attains the Singleton bound with equality, i.e. it is MDS.

2. Consider the code $\mathcal{D}$, whose generator matrix is $\boldsymbol{H}'$. We already proved that all rows of $\boldsymbol{H}'$ are linearly independent. We have that the length of $\mathcal{D}$ is $n+1$ and the dimension is $n-k$.

   We showed in the practice session that the dual code of an MDS code is also MDS. We have that $\mathcal{D}$ is dual of $\mathcal{C}'$, which is MDS. Therefore, $\mathcal{D}$ is also MDS. Its distance is $(n+1)-(n-k)+1=k+2$.

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 given by

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

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 $v_2 = v_4 = v_6 = 6$.

Assume that $\bar{\boldsymbol{c}} \in \mathcal{C}$ is transmitted, and $\bar{\boldsymbol{y}} = (1, 5, 2, 3, 4, 6) \in (\mathbb{F})^6$ 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 $\bar{\boldsymbol{c}} \in \mathcal{C}$.

Solution: Before proceeding further, let us re-write $\boldsymbol{H}$ modulo 7:

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

(a) Syndrome vector:

$$\bar{\boldsymbol{s}} = \boldsymbol{H}\bar{\boldsymbol{y}}^{\mathsf{T}} = \begin{pmatrix} 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 5 & 3 & 3 & 5 & 1 \\ 1 & 3 & 2 & 5 & 4 & 6 \\ 1 & 6 & 6 & 6 & 6 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \\ 2 \\ 3 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 91 \\ 67 \\ 87 \\ 91 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 3 \\ 0 \end{pmatrix}$$

Therefore, the syndrome polynomial is

$$S(x) = 3x^2 + 4x$$

(b) We use the extended Euclid's algorithm. Initialization:

$$\begin{aligned} r_{-1}(x) = a(x) = x^{d-1} = x^4 \qquad & t_{-1}(x) = 0 \\ r_0(x) = b(x) = S(x) = 3x^2 + 4x \qquad & t_0(x) = 1. \end{aligned}$$

Iterations of the extended Euclid's algorithm are as follows.

Iteration 1:

$$\begin{aligned} r_{-1}(x) = x^4 &= \underbrace{(5x^2 + 5x + 5)}_{q_1(x)} \cdot (3x^2 + 4x) + \underbrace{(x)}_{r_1(x)} \\ t_{-1}(x) = 0 &= (5x^2 + 5x + 5) \cdot (1) + \underbrace{(2x^2 + 2x + 2)}_{t_1(x)} \end{aligned}$$

We observe that $\deg r_1 = 1 < \frac{d-1}{2} = \frac{5-1}{2} = 2$. Thus, we stop iterations.

We set $\Lambda(x) = t_1(x) = 2x^2 + 2x + 2$ and $\Gamma(x) = r_1(x) = x$. We notice that $\Lambda(0) = 2 \neq 1$.

Therefore $\Lambda(x) \leftarrow 2^{-1} \cdot \Lambda(x) = x^2 + x + 1$ and $\Gamma(x) \leftarrow 2^{-1} \cdot \Gamma(x) = 4x$.

(c) To find locations of errors, we need to find roots of $\Lambda(x)$. By trying different elements of $\mathbb{F}_7$, we find the roots: $\{2, 4\}$. Therefore, there are errors in positions j where $\alpha_j^{-1} \in \{2, 4\}$. In other words, $\alpha_j \in \{4, 2\}$ and $j \in \{4, 2\}$. That is, the errors are in positions 2 and 4.

Since $\Lambda'(x) = 2x + 1$, we obtain values of errors:

$$\begin{aligned} e_2 &= -\frac{\alpha_2}{v_2} \cdot \frac{\Gamma(\alpha_2^{-1})}{\Lambda'(\alpha_2^{-1})} = -\frac{2}{6} \cdot \frac{2}{1+1} = -2.6 = -5 = 2, \\ e_4 &= -\frac{\alpha_4}{v_4} \cdot \frac{\Gamma(\alpha_4^{-1})}{\Lambda'(\alpha_4^{-1})} = -\frac{4}{6} \cdot \frac{1}{4+1} = -\frac{4}{6} \cdot 3 = -2 = 5. \end{aligned}$$

(d) If we assume the aforementioned number of errors then

$$\bar{\boldsymbol{c}} = \bar{\boldsymbol{y}} - \bar{\boldsymbol{e}} = (1, 5, 2, 3, 4, 6) - (0, 2, 0, 5, 0, 0) = (1, 3, 2, 5, 4, 6).$$

(e) Verification:

$$\boldsymbol{H}\bar{\boldsymbol{c}}^{\mathsf{T}} = \begin{pmatrix} 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 5 & 3 & 3 & 5 & 1 \\ 1 & 3 & 2 & 5 & 4 & 6 \\ 1 & 6 & 6 & 6 & 6 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \\ 2 \\ 5 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 91 \\ 63 \\ 91 \\ 91 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$