+1/1/60+

EPFL

Prof. M. Gastpar

Quiz 6 (Homeworks 12 & 13)

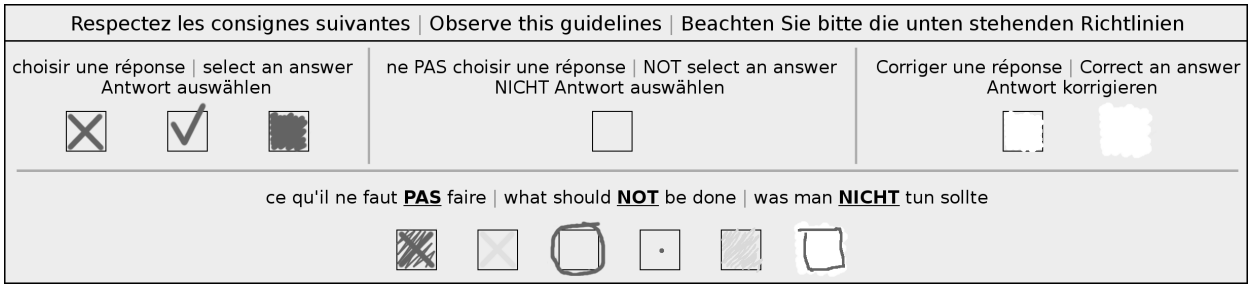
Due on Moodle

on Monday, May 26, 2025, at 23:59.

Quiz 6

SCIPER : **111111**

- This quiz is to be solved individually.
- Try not to use any of the course materials other than the formula collection on a first attempt.
- Once you are done, enter your answers into Moodle. Moodle will give you feedback. You can update your answers as many times as you want before the deadline.
- For each question there is **exactly one** correct answer. We assign **negative points** to the **wrong answers** in such a way that a person who chooses a wrong answer loses **25 %** of the points given for that question.



For your examination, preferably print documents compiled from auto-multiple-choice.

Question 1

[0 points] *Note: This is an* **open** *question. In the real exam, we will grade your arguments. Here for the quiz, we do not have the capacity to do this. Therefore, you will merely enter your final answer into a multiple choice grid on Moodle. However, do make sure to carefully look at the solution and compare to your answer. How many points would you have given yourself?*

Let $\mathcal{C}$ be a (n, k) linear block code over $\mathbb{F}_2$ of block length n such that n is even and minimum distance $d_{min} = 3$. We construct a new code $\mathcal{C}'$ by appending onto each codeword $\vec{x} \in \mathcal{C}$ three parity bits as follows:

$x_{n+1} = x_1 \oplus x_3 \oplus x_5 \oplus \ldots \oplus x_{n-1}$,

$x_{n+2} = x_2 \oplus x_4 \oplus x_6 \oplus \ldots \oplus x_n$,

$x_{n+3} = x_1 \oplus x_2 \oplus x_3 \oplus \ldots \oplus x_n$.

The goal is to find the minimum distance d'_{min} of the new $(n + 3, k)$ linear block code. Could it happen that $d'_{min} = 3$, $d'_{min} = 4$, $d'_{min} = 5$ or $d'_{min} = 6$? For each case, if it is possible, give conditions under which it can happen. If it is not possible, argue why not.

Solution:

- This problem is about leveraging the theorem that in linear codes, *the minimum distance is equal to the minimum weight.* This means that the original code has at least one codeword of weight 3.
- First of all, this theorem directly implies that the new minimum distance *cannot be smaller* than the original minimum distance, i.e., $d'_{min} \geq d_{min} = 3$ (since adding additional parities cannot reduce the weight of any codeword).
- Next, clearly, the minimum distance cannot go up by more than 3: We are only adding three new positions to every codeword. Since in the original code, there is a codeword of weight three, adding three more positions to the codeword can at best increase the weight to 6. Hence, $d'_{min} \leq 6$.
- Now, it becomes more subtle. Let us start by checking if there is a way to get $d'_{min} = 6$. The only way for this to happen would be if in the original codeword, the parity of the bits in even positions, the parity of the bits in odd positions, and the parity of the bits in all positions are all equal to one. Obviously, this is not possible: For example, if the even- and the odd-position parity are both one, the the parity of all bits must be zero. Hence, we can rule out $d'_{min} = 6$.
- Next, could we have $d'_{min} = 5$? Here, the answer is indeed yes. For example, the original code is such that in even positions, codewords are always zero, and only odd positions may be non-zero. Moreover, suppose that the code does not have any weight-4 codewords. Now, the minimum-weight codewords have three ones, all of them is odd positions. Clearly, this means that $x_{n+1} = x_{n+3} = 1$ (and $x_{n+2} = 0$). Hence, all original weight-3 codewords are now of weight 5. Since by assumption, there are no weight-4 codewords, the new code thus has $d'_{min} = 5$.
- Then, could we have $d'_{min} = 3$? Since $d_{min} = 3$, if $d'_{min} = 3$, then there must exists some codeword of weight-3 such that $x_{n+1} = x_{n+2} = x_{n+3} = 0$. If for all codeword of weight-3, three ones are in odd positions, then we know $d'_{min} = 5$. If there exists a codeword of weight-3 such that three ones are in

even positions, then it is the same story. If two of them are in odd positions, and one of them is in even position, or vise versa, we find that in any case at least two of the added bits are ones for a weight-3 codeword. Therefore, $d'_{min} = 3$ is not possible.

- Finally, could we have $d'_{min} = 4$? Here, the answer is also yes. For example, there exists some codeword of weight-4 in the original code such that two ones are in even positions, and two ones are in odd positions. Thus, $x_{n+1} = x_{n+2} = x_{n+3} = 0$, and the new code now has at most minimum distance 4. In addition, any weight-3 codeword in the original code has weight at least 5. Hence, in this case, the minimum distance $d'_{min} = 4$.

Question 2:

[5 points] Let $G_i, i \in \{1, \ldots, 8\}$, be valid generator matrices of dimensions $\mathbb{F}^{k_i \times n_i}$, all over the same field $\mathbb{F}$. Which of the following are always valid generator matrices?
Hint: recall that "valid" means that for all i, $k_i \leq n_i$ and rank$(G_i) = k_i$.

$\begin{pmatrix} G_1 \\ \hline G_2 \end{pmatrix}$ where $n_1 = n_2$ and $k_1 + k_2 \leq n_1$.

☐ TRUE ■ FALSE

Solution: One counterexample is that $G_1 = G_2$, and clearly the rank is $k_1 < k_1 + k_2 = 2k_1$.

$\left(\begin{array}{c|c|c} G_3 & G_4 & 0 \\ \hline & 0 & G_5 \end{array}\right)$ where $k_3 = k_4 + k_5$.

■ TRUE ☐ FALSE

Solution: The new matrix is the concatenation $[G_3; A]$, which has rank at least rank(G_3). Since G_3 is a generator matrix, its rank is equal to the number of its rows k_3, which is also the number of rows of the new matrix.

$D_1 \cdot G_6 \cdot D_2$, where $D_1 \in \mathbb{F}^{k_6 \times k_6}$ and $D_2 \in \mathbb{F}^{n_6 \times n_6}$ are diagonal matrices with non-zero diagonal elements.

■ TRUE ☐ FALSE

Solution: The new matrix still has the same number of rows as G_6, and the rank of the new matrix is also unchanged as rank(G_6).

$G_7 + G_8$ with $k_7 = k_8$ and $n_7 = n_8$.

☐ TRUE ■ FALSE

Solution: One counterexample is that $G_7 + G_8 = 0_{k_7 \times n_7}$.

Question 3:

[5 points] Let

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

be the generator matrix of a $(6, 4)$ linear code $\mathcal{C}$ over $\mathbb{F}_2$.

Answer the following true/false questions.

G admits a systematic form (i.e., it can be put into systematic form via elementary row operations).

☐ TRUE ■ FALSE

Solution: After some elementary row operations, we find that its reduced row echelon form is

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

which cannot be written in a systematic form which is the concatenation of the identity matrix and some other matrix.

$d_{min} = 2$.

☐ TRUE ■ FALSE

Solution: As we can see from its row echelon form, some of the codewords are of weight 1. So the minimum distance of this code is 1.

If one substitutes the last row of G by $(1, 0, 0, 1, 1, 1)$, the thereby obtained matrix generates the same code $\mathcal{C}$.

■ TRUE ☐ FALSE

Solution: $(1, 0, 0, 1, 1, 1)$ is a linear combination of the original last row $(0, 1, 1, 1, 0, 1)$ and the first row $(1, 1, 1, 0, 1, 0)$, and hence, replacing the last row with $(1, 0, 0, 1, 1, 1)$ won't change the subspace spanned by the original four rows in G.

Performing an arbitrary column permutation on G yields a generator matrix of a linear code with the same parameters n, k, d_{min}.

■ TRUE ☐ FALSE

Solution: Apparently, column permutation on G won't change n. Also, its rank stays the same, as the columns still span the same subspace. Then, the reduced row echelon form of the new matrix G' is the matrix obtained by applying the same column permutation on the reduced row echelon form of G. This will not change the weight of each codeword.

For your examination, preferably print documents compiled from auto-multiple-choice.

Question 4:

[5 points] Let $\mathcal{C}_1$ be a linear code over $\mathbb{F}_3^n$, and let $\mathcal{C}_2$ be a linear code over $\mathbb{F}_2^n$. Answer the following true/false questions.

$\mathcal{C}_1 \cup \mathcal{C}_2$ is necessarily a linear code over $\mathbb{F}_3^n$.

☐ TRUE ■ FALSE

Solution: The point was for students to try out a few simple codes. For example, let $\mathcal{C}_1 = \{00, 11\}$ and $\mathcal{C}_1 = \{00, 10, 20\}$. Then, their union is simply the collection of all their codewords, $\mathcal{C}_1 \cup \mathcal{C}_2 = \{00, 11, 10, 20\}$. In this example, we observe that $\mathcal{C}_1$ and $\mathcal{C}_2$ are linear, but their union is clearly not a linear code.

$\mathcal{C}_1 \cap \mathcal{C}_2$ is necessarily a linear code over $\mathbb{F}_2^n$.

☐ TRUE ■ FALSE

Solution: Likewise, the point was for students to try out a few simple codes. For example, let $\mathcal{C}_1 = \{00, 11\}$ and $\mathcal{C}_1 = \{00, 10, 20\}$. Then, their (set) intersection is $\mathcal{C}_1 \cap \mathcal{C}_2 = \{00\}$. So, this example is not very helpful yet. Some more scribbling, we find the example $\mathcal{C}_1 = \{000, 110, 011, 101\}$ and $\mathcal{C}_2 = \{000, 110, 011, 121, 220, 022, 212, 102, 201\}$, which are both linear codes (over their respective fields). Their (set) intersection is $\mathcal{C}_1 \cap \mathcal{C}_2 = \{000, 110, 011\}$, which is clearly not a linear code.

Question 5

[5 points] Let $\mathcal{C}_1$ be a (n_1, k) linear block code over $\mathbb{F}_p$ with p prime and $|\mathcal{C}_1| = 27$. Let $\mathcal{C}_2$ be a (n_2, k) linear block code over $\mathbb{F}_2$ of the same dimension k. Which of the following is true?

☐ $|\mathcal{C}_2| = 27$

■ $|\mathcal{C}_2| = 8$

☐ $|\mathcal{C}_2| = 21$

☐ $|\mathcal{C}_2| = 16$

Solution: The number of codewords in a binary linear block code over a prime field $\mathbb{F}_p$ must be of the form p^k. Of course, $27 = 3^3$. So we must have $p = 3$ and $k = 3$. A binary linear block code with $k = 3$ has $2^3 = 8$ codewords.