EXERCISES N° 1, BASIC NOTIONS, WITH SOLUTIONS

Exercise 1 (A short quizz)**.** Let $C \subseteq \mathbb{F}_q^n$ be an $[n,k,d]$ code and Gm, H be respectively a generator and a parity check matrix of C. In what follow we list operations on G yielding a new matrix G'. For any one:

- does G' generate the same code?
- if not,
  - has the new code generated by G' the same length?
  - a larger dimension?
  - a smaller dimension?
  - might this code have a larger minimum distance?
  - a smaller minimum distance?

(1) Removing a row;
(2) swapping two rows;
(3) removing a column;
(4) swapping two columns;
(5) adding an additional row drawn at random;
(6) adding an additional row defined as the sum of all the other rows;
(7) adding an additional column defined as the sum of all the other columns.

Same questions when the operations are applied to H.

Exercise 2 ($(u|u+v)$ construction)**.** Let C, C' be two codes of respective parameters $[n,k,d]_q$ and $[n,k',d']_q$ with $d' \geqslant 2d$. We consider the code C'' defined as:

$$C'' = \{(u \mid u+v), \text{ such that } u \in C,\ v \in C'\}$$

where "$|$" denotes the concatenation of words. Prove that C'' has parameters $[2n, k+k', 2d]$.

Exercise 3 (Product of codes)**.** $\star$ Given two codes $C, C' \subseteq \mathbb{F}_q^n$, the product $C \otimes C'$ is defined as

$$C \otimes C' := \mathbf{span}_{\mathbb{F}_q}\{(c_1c_1', \dots, c_1c_n', c_2c_1', \dots, c_2c_n', \dots, c_nc_1', \dots, c_nc_n'), \text{ such that}, c \in C,\ c' \in C'\}.$$

A far more comfortable way to see them is to see codewords of $C \otimes C'$ as $n \times n$ matrices and for this point of view:

$$C \otimes C' = \mathbf{span}_{\mathbb{F}_q}\{c^T \cdot c' \mid c \in C,\ c' \in C'\},$$

where the ^{T} stands for the matrix transposition.

(1) Prove that $C \otimes C'$ equals the space of matrices whose rows are in C' and columns are in C.
(2) Prove that $C \otimes C'$ is $[n^2, kk', dd']$ and that its miniumum weight codewords are of the form $c^T \cdot c'$ where c has weight d and c' has weight d'.

Exercise 4 (The linear Gilbert Varshamov bound)**.** $\star$

(1) Let $0 < k < n$. Compute the number rank k matrices $\mathfrak{M}_{k\times n}(\mathbb{F}_q)$.

Indication: The first row of such a matrix can be any nonzero vector of $\mathbb{F}_q^n$, the second one can be any arbitrary vector non collinear to the first one... the i-th one can be any arbitrary vector out of the spam of the $(i-1)$ previous ones...

(2) Given a code C of parity-check matrix H, prove that the minimum distance d is the smallest integer ℓ such that there exist ℓ distinct columns of H which are non collinear.

(3) Prove that if

$$q^n \geqslant q^k \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i,$$

Then, there exists a k–dimensional code C of length n and distance $\geqslant d$.

Indication : We will construct iteratively a parity-check matrix of C, first construct an invertible $(n-k)\times(n-k)$ matrix. Then, add columns which forms a linearly independent family with any $d-2$ other column vectors among those previoulsy constructed. The above bound is there to assert the existence of such an additional column.

Exercise 5 (Solution to Exercise 1)**.** (1) Removing a row changes the code and provides a new code C' of the same length which is a subcode of C. Hence the dimension could be reduced by one unless G was not full rank and the deleted row was a linear combination of the other ones. In terms of minimum distance, the new code is a subcode and hence might have a larger minimum distance. The minimum distance is at least the same.

(2) swapping two rows does not change the code : the code is generated by the rows of the matrix. No matter how they are sorted.

(3) removing a column changes the code and provides a new code C' of length $n-1$. The new code has the same dimension unless the i–th column has been removed and C contained the codeword of weight 1:

$$(0 \ \cdots \ 0 \ 1 \ 0 \ \cdots \ 0)$$

where the 1 is at the i–th position. In terms of minimum distance, if C has minimum weight codewords with a nonzero entry at the deleted position, then the new code C' has codewords of weight $d-1$ but not less if not, the minimum weight codewords of C' remains d. Hence the new code C' has a minimum distance d' which is either $d-1$ or d.

(4) swapping two columns changes the code and provides a new code C' of the same length n. The new code is obtained by the map consisting in swapping entries at a position i and a position j. This map is bijective and preserves the Hamming weight (it is an isometry with respect to the Hamming distance). Hence, C' has the same dimension and minimum distance.

(5) adding an additional row drawn at random provides a new code C' of the same length and that contains C. If the new row is in C and hence is a linear combination of the rows of G, then $C' = C$ else $C \subsetneq C'$ and C' has dimension $k+1$ and its minimum distance is at most d but might be less.

(6) adding an additional row defined as the sum of all the other rows does not change the code since the new row is a linear combination of the other ones and hence the space spanned by the rows remains the same.

(7) adding an additional column defined as the sum of all the other columns changes the code and provides a new code C' of length $n+1$. This new code is obtained from C by joining at the end of any codeword the sum of its entries. The dimension of C' is still k since the rank of G is unchanged. In terms of minimum distance, the minimum distance is unchanged if there are minimum weight codewords whose sum of entries is zero. If not, then the minimum distance is $d+1$.

Same questions when the operations are applied to H:

(1) Removing a row of H changes the code and provides a new code C' of the same length which contains of C. Hence the dimension could be increased by one unless H was not full rank and the deleted row was a linear combination of the other ones. In terms of minimum distance, the new code contains C and hence might have a smaller minimum distance. The minimum distance is at most the same.

(2) swapping two rows does not change the code.

(3) removing a column changes the code and provides a new code C' of length $n-1$. If the i–th column of H is removed, the new code is obtained from C by keeping only the codewords whose i–th entry is zero and by removing this entry. It is the *shortening of* C at position i.

This new code has dimension $k-1$ unless the i–th column has been removed and any codeword in C has its i–th entry equal to 0.

In terms of minimum distance, C' is constructed from the subcode of C of words whose i–th entry is 0. Therefore, the minimum distance of C' is at least d and might be larger.

(4) swapping two columns changes the code and provides a new code C' of the same length n. The new code is obtained by the map consisting in swapping entries at a position i and a position j exactly as in the case of swapping columns of a generator matrix.

(5) adding an additional row drawn at random provides a new code C' of the same length and that is contained in C. If the new row is in C and hence is a linear combination of the rows of G, then $C' = C$ else $C \subsetneq C'$ and C' has dimension $k-1$ and its minimum distance is at least d but might be larger.

(6) adding an additional row defined as the sum of all the other rows does not change the code since the new row is a linear combination of the other ones and hence the space spanned by the rows remains the same.

(7) adding an additional column defined as the sum of all the other columns changes the code and provides a new code C' of length $n+1$. This new code is obtained from C by joining at the end of any codeword the entry 0 and adding as an additional generator the codeword $(1\ 1\ \cdots\ 1)$. The dimension of C' is still k since the rank of H is unchanged. In terms of minimum distance, the minimum distance is at most d but might be less.

Solution for Exercise 2

The dimension. Consider the map

$$\phi \left\{ \begin{array}{ccc} C \times C' & \longrightarrow & C'' \\ (u,v) & \longmapsto & (u|u+v) \end{array} \right. .$$

This is a linear map an it is injective. Indeed, if $\phi((u,v)) = 0$ then $(u|u+v) = 0$ which entails that $u = v = 0$. Since C'' is also defined as the image of ϕ, this map is an isomorphism and hence

$$\dim C'' = \dim C + \dim C'.$$

The minimum distance. Let $c'' = (c|c+c') \in C'' \setminus \{0\}$. First consider elementary cases:

- If $c = 0$, then $w_H(c'') = w_H(c') \geqslant d'$, by definition of d'.
- If $c' = 0$, then $w_H(c'') = 2w_H(c) \geqslant 2d$, by definition on d.

Since we assumed that $d' \geqslant 2d$, in both situations c'' has weight $\geqslant 2d$. Now, assume that $c \neq 0$ and $c' \neq 0$. Let introduce a notation. For all $x \in \mathbb{F}_q^n$, we call the *support* of x:

$$\mathbf{supp}\,(x) := |\{i \mid x_i \neq 0\}|.$$

In particular, $w_H(x) = |\mathbf{supp}\,(x)\,|$. Let $c'' = (c|c+c') \in C''$ with $c, c' \neq 0$. Then, we have

$$w_H(c+c') \geqslant |\mathbf{supp}\,(c)\,| + |\mathbf{supp}\,(c')\,| - 2|\mathbf{supp}\,(c) \cap \mathbf{supp}\,(c')\,| \tag{1}$$

and $|\mathbf{supp}\,(c) \cap \mathbf{supp}\,(c')\,| \leqslant \min\{w_H(c), w_H(c')\}$. Hence

$$w_H(c+c') \geqslant w_H(c) + w_H(c') - 2\min\{w_H(c), w_H(c')\}.$$

Therefore,

$$w_H(c'') \geqslant 2w_H(c) + w_H(c') - 2\min\{w_H(c), w_H(c')\}.$$

If $w_H(c) \leqslant w_H(c')$, then
$$w_H(c'') \geqslant w_H(c') \geqslant d'.$$
Else, if $w_H(c) \geqslant w_H(c')$, then
$$w_H(c'') \geqslant 2w_H(c) - w_H(c') \geqslant w_H(c') \geqslant d'.$$

Remark 1. Let c be a codeword of C of weight d, then $(c|c)$ has weight $2d$, which proves that the minimum distance is actually exactly $2d$.

Remark 2. Equation (1) is an equality if the code is binary, i.e. if it is defined over $\mathbb{F}_2$.

Solution to Exercise 3

(1) Let E be the vector space of matrices $n \times n$ matrices whose rows are in C' and columns are in C. Clearly $C \otimes C' \subseteq E$. We prove the converse inclusion. Let $M \in E$ and let $c'_1 \in C'$ and $c_1 \in C$ be respectively the first row and first column of M. Then the matrix
$$M_1 \stackrel{\text{def}}{=} M - c_1^T \cdot c'_1 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & M' & \\ 0 & & \end{pmatrix}$$
is also in E and if we denote by c'_2, c_2 the second row and column of M_1, then $M_2 \stackrel{\text{def}}{=} M_1 - c_2^T c'_2$ is in E and has the two first rows and columns equal to zero. By induction, we get
$$M - c_1^T c'_1 - c_2^T c'_2 - \cdots - c_s^T c'_s = 0$$
for some integer $s > 0$. This proves that $M \in C \otimes C'$.

(2) **The dimension.** It is a classical result on tensor products, but let us give an ad hoc proof. Let $g_1, \ldots, g_k$ and $g'_1, \ldots, g'_{k'}$ be respective bases for C and C'. We will prove that $\left(g_i^T g'_j\right)_{i,j}$ is a basis of $C \otimes C'$. It is clearly a family of generators. We will prove that they are linearly independent. Let $(\lambda_{ij})_{i,j \in \{1 \ldots k\} \times \{1 \ldots k'\}}$ be scalars such that

$$\sum_{i,j} \lambda_{ij} g_i^T g'_j = 0. \tag{2}$$

Since the g_i's form a basis, for all $\ell \in \{1, \ldots, k\}$, there exists a linear form $\varphi_\ell : C \to \mathbb{F}_q$ such that
$$\varphi_\ell(g_i) = \begin{cases} 1 & \text{if} \quad i = \ell \\ 0 & \text{else.} \end{cases}$$
Let $\tilde{\varphi}_\ell : C \otimes C' \to C'$ be defined on elementary products $c^T c'$ by:
$$\forall (c, c') \in C \times C', \ \tilde{\varphi}_\ell(c^T c') \stackrel{\text{def}}{=} \varphi_\ell(c).c'$$
and extended by linearity. Then, applying $\tilde{\varphi}_\ell$ to (2),
$$\tilde{\varphi}_\ell \left(\sum_{i,j} \lambda_{ij} g_i^T g'_j \right) = 0$$

and by definition of $\tilde{\varphi}_i$ we get,

$$\sum_{j=1}^{k'} \lambda_{\ell j} g'_j = 0.$$

Since the g'_j form a basis of C', we get that $\lambda_{\ell j} = 0$ for all $j \in \{1, \dots, k\}$ and this can be done for all $\ell \in \{1, \dots, k\}$. Thus, the $g_i^T g'_j$'s are linearly independent, which proves that $C \otimes C'$ has dimension kk'.

The minimum distance. Let $M \in C \otimes C' \setminus \{0\}$. Notice first that M has at least d' nonzero columns. Indeed, if it had strictly less that d' nonzero columns, then there would exist a nonzero row (since M is nonzero it has at least one nonzero row) and this row is a codeword of C' which would be of weight $< d'$, which contradicts the definition of the minimum distance d'. Therefore, M has at least d' nonzero columns and since every column is in C, each nonzero column has weight greater than or equal to d, which yields $w_H(M) \geqslant dd'$. Thus, the minimum distance of $C \otimes C'$ is at least dd'.

Finally, let $c \in C$ be a codeword of weight d and $c' \in C'$ a codeword of weight d' then $c^T c' \in C \otimes C'$ has weight dd', which concludes the proof that dd' is the minimum distance of $C \otimes C'$.

Minimum weight codewords. Let M be a codeword of $C \otimes C'$ of weight dd'. One proves easily that M has exactly d nonzero rows and d' nonzero columns (else its weight would be $> dd'$). Let c be a nonzero column and c' a nonzero row of M. Then, one checks easily that M and $c^T c'$ have the same support and that

$$w_H(M - c^T c') < dd',$$

and by definition of the minimum distance, this entails that $M - c^T c' = 0$, thus, $M = c^T c'$, which concludes the proof.

Solution to Exercise 4

(1) We have $q^n - 1$ choices for the first row (every choice but the zero vector). The second row must be non collinear to the first one, which yields $q^n - q$ choices and so on... for the i–th row, it must be out of the $(i-1)$–dimensional vector space spanned by the $i-1$ first rows, which yields $q^n - q^{i-1}$ possible choices. As a conclusion, the number of such matrices is

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{i-1}) \cdots (q^n - q^{k-1}).$$

(2) One just has to notice that a codeword $c \in C$ is an element of the kernel of H and hence it induces a linear relation between the columns of H. The number of columns involved in the linear relation is nothing but the weight of c.

(3) Let us first choose for the first $n-k$ columns an arbitrary matrix of $\mathbf{GL}(n-k, \mathbb{F}_q)$. Such a matrix exists since, from question 1, there exist $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) > 0$ such matrices. Now the $n-k+1$-th column should be chosen so that no $d-1$

columns (or less) are linearly linked. Thus, the $n-k+1$-th column should not be linked with any $d-2$ (or less) of the $n-k$ first one. There are

$$\sum_{i=1}^{d-2}(q-1)^i\binom{n-k}{i}$$

such linear combinations. Thus, if

$$q^{n-k} > \sum_{i=1}^{d-2}(q-1)^i\binom{n-k}{i},$$

one can choose a $(n-k+1)$-th column so that no $d-1$ of them are linearly linked. By induction, the construction of the j-th column, is possible if

$$q^{n-k} > \sum_{i=1}^{d-1}(q-1)^i\binom{n-k+(j-1)}{i}.$$

Then, notice that the map

$$j \longmapsto \sum_{i=1}^{d-1}(q-1)^i\binom{n-k+(j-1)}{i}$$

is increasing, thus, if

$$q^{n-k} > \sum_{i=1}^{d-1}(q-1)^i\binom{n-1}{i}.$$

then, the columns $n-k+1$ to n can be chosen, which yields the result.