EXERCISES N° 1, BASIC NOTIONS

Note. Exercises marked with a $\star$ are more difficult.

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

$$C \otimes C' := \mathbf{span}_{\mathbb{F}_q}\{(c_1c'_1, \ldots, c_1c'_n, c_2c'_1, \ldots, c_2c'_n, \ldots, c_nc'_1, \ldots, c_nc'_n),\ \text{such that},\ c \in C,\ c' \in C'\}.$$

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)**.** ⋆

(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.