Mid-term exam, November 29, 2023

You have 1h30. You can write your answers either in French or in English.

Notes.
— *In any exercise, any code is linear.*
— *Questions marked with a (⋆) are harder than the other ones.*

Exercise 1. A code $\mathscr{C} \subseteq \mathbb{F}_q^n$ of dimension k is said to be *systematic* if it has a generator matrix of the form

$$\left(\mathbf{I}_k \quad | \quad \mathbf{R} \right),$$

for some matrix $\mathbf{R} \in \mathbb{F}_q^{k\times(n-k)}$ and where $\mathbf{I}_k$ denotes the $k \times k$ identity matrix.

1. Prove that a code $\mathscr{C} \subseteq \mathbb{F}_q^n$ with generator matrix $\mathbf{G}$ is systematic if and only if the k leftmost columns of $\mathbf{G}$ are linearly independent.
2. Prove that $(\ -\mathbf{R}^\top \mid \mathbf{I}_{n-k})$ is a parity check matrix of $\mathscr{C}$.
3. Give an example of non systematic code of length 4 and dimension 2 over $\mathbb{F}_2$.

For any permutation $\sigma \in \mathfrak{S}_n$ (the permutation group over n elements), denote by $\mathbf{P}_\sigma$ the corresponding permutation matrix. Then, for a code $\mathscr{C}$, denote by $\mathscr{C}\mathbf{P}_\sigma$ the *permuted code* defined by

$$\mathscr{C}\mathbf{P}_\sigma \stackrel{\text{def}}{=} \{\mathbf{c}\mathbf{P}_\sigma \mid \mathbf{c} \in \mathscr{C}\}.$$

4. Prove that for any linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$, there exists $\sigma \in \mathfrak{S}_n$ such that $\mathscr{C}\mathbf{P}_\sigma$ is systematic.
5. Prove that an $[n, k, n-k+1]$–code (*i.e.* a code achieving Singleton bound) is systematic.
6. Prove that a cyclic code is systematic.

A code of length $n = 2n_0$ for some positive integer n_0 is doubly circulant if it is stable by a "double cyclic shift". *i.e.*, it has a generator matrix of the form :

$$\left(\begin{array}{ccccc|ccccc}
f_0 & f_1 & \cdots & \cdots & f_{n_0-1} & g_0 & g_1 & \cdots & \cdots & g_{n_0-1} \\
f_{n_0-1} & f_0 & f_1 & \cdots & f_{n_0-2} & g_{n_0-1} & g_0 & g_1 & \cdots & g_{n_0-2} \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & f_1 & \vdots & & \ddots & \ddots & g_1 \\
f_1 & f_2 & \cdots & f_{n_0-1} & f_0 & g_1 & g_2 & \cdots & g_{n_0-1} & g_0
\end{array}\right).$$

Similarly to cyclic codes, doubly circulant codes can be represented as a pair of polynomials $(f(X), g(X)) \in (\mathbb{F}_q[X]/(X^{n_0}-1))^2$. In particular, any element of the code is represented by a pair $(u(X)f(X) \mid u(X)g(X))$ for some $u \in \mathbb{F}_q[X]/(X^{n_0}-1)$.

Turn the page please ⟶

7. ($\star$) Prove that a doubly circulant code defined by the pair $(f(X), g(X)) \in (\mathbb{F}_q[X]/(X^{n_0}-1))^2$ has dimension n_0 if and only if $\gcd(f, g, X^{n_0}-1) = 1$.

   Hint. One could consider the map

$$\left\{ \begin{array}{ccc} \mathbb{F}_q[X]/(X^{n_0}-1) & \longrightarrow & \mathscr{C} \\ u(X) & \longmapsto & (u(X)f(X)) \mid u(X)g(X)) \end{array} \right.$$

   which turns out to be injective if and only if the code has dimension n_0.

8. ($\star$) Prove that a doubly circulant code defined by the pair $(f(X), g(X)) \in (\mathbb{F}_q[X]/(X^{n_0}-1))^2$ is systematic if and only if f is invertible in $(\mathbb{F}_q[X]/(X^{n_0}-1))^2$.

Exercise 2. Let n be a positive integer prime to q. Let $\mathscr{C}, \mathscr{D} \subseteq \mathbb{F}_q^n$ be cyclic codes with generating polynomials $g_{\mathscr{C}}, g_{\mathscr{D}}$ which both divide $(X^n - 1)$ and cyclotomic classes $I_C, I_D \subseteq \mathbb{Z}/n\mathbb{Z}$.

1. (a) Prove that $\mathscr{C} \cap \mathscr{D}$ is cyclic;
   (b) express its generating polynomial in terms of $g_{\mathscr{C}}, g_{\mathscr{D}}$;
   (c) express its cyclotomic classes in terms of I_C, I_D.
2. Same questions ((a), (b), (c)) for $\mathscr{C} + \mathscr{D}$.
3. ($\star$) Consider the code

$$\mathscr{E} \stackrel{\text{def}}{=} \operatorname{Span}_{\mathbb{F}_q}\{(u(X)v(X)) \mid u \in \mathscr{C},\ v \in \mathscr{D}\},$$

   where the product is performed in the ring $\mathbb{F}_q[X]/(X^n - 1)$, and the code

$$\mathscr{F} \stackrel{\text{def}}{=} \{(g_{\mathscr{D}}(X)u(X)) \mid u(X) \in \mathscr{C}\}.$$

   Prove that both $\mathscr{E}$ and $\mathscr{F}$ equal $\mathscr{C} \cap \mathscr{D}$.
   Hint. One can first suppose that $g_{\mathscr{C}}$ and $g_{\mathscr{D}}$ are prime to each other.

Exercise 3. For a vector $\mathbf{c} \in \mathbb{F}_q^n$ denote by $\operatorname{Supp}(\mathbf{c})$ the set $\operatorname{Supp}(\mathbf{c}) \stackrel{\text{def}}{=} \{i \in \{1, \ldots, n\} \mid c_i \neq 0\}$. Given a linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ and $I \subseteq \{1, \ldots, n\}$, we denote by

$$\mathscr{C}_{|I} \stackrel{\text{def}}{=} \{\mathbf{c} \in \mathscr{C} \mid \operatorname{Supp}(\mathbf{c}) \subseteq I\}.$$

For a positive integer $r \leqslant n$, the r–*th generalised Hamming weight* of $\mathscr{C}$ is defined as

$$d_r(\mathscr{C}) \stackrel{\text{def}}{=} \min\{\sharp I \mid I \subseteq \{1, \ldots, n\} \quad \text{and} \quad \dim \mathscr{C}_{|I} = r\}.$$

1. Prove that $d_1(\mathscr{C})$ is nothing but the minimum distance.
2. Let k be the dimension of $\mathscr{C}$, prove that

$$1 \leqslant d_1(\mathscr{C}) < d_2(\mathscr{C}) < \cdots < d_k(\mathscr{C}) \leqslant n.$$

3. Prove that for an $[n, k]$ code and any $r \leqslant k$, we have

$$d_r(\mathscr{C}) \leqslant n - k + r.$$

4. Deduce the sequence of generalised Hamming weights for a code achieving Singleton bound.