Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$. We denote by k its dimension. For any word $c \in \mathbb{F}_q^n$, we denote by $c(x) = \sum_{i=0}^{n-1} c_i x^i$ the associated polynomial.

Let G be a generator matrix of $\mathcal{C}$ whose rows are denoted by g_i. We also denote by $s(x)$ the monic gcd of all the $g_i(x)$.

If $\mathcal{C}$ is cyclic, we recall that there exists a unique monic polynomial $g(x)$ of degree $n-k$ such that

$$\mathcal{C} = \{c \in \mathbb{F}_q^n \mid \exists a(x) \in \mathbb{F}_q[x], \deg a(x) < k \text{ and } c(x) = a(x)g(x)\}$$

We now prove the following result.

Proposition. *$\mathcal{C}$ is a cyclic code if and only if the following properties are satisfied:*

(i) $\deg s(x) = n - k$*;*

(ii) for all $i \in [0, k-1]$*, the word corresponding to the polynomial* $x^i s(x)$ *lies in* $\mathcal{C}$*.*

Moreover, if $\mathcal{C}$ is cyclic, we have $s(x) = g(x)$.

Proof.

• Assume $\mathcal{C}$ is a cyclic code. On the one hand, $g \in \mathcal{C}$ implies there exist some $(\lambda_i)_i \in \mathbb{F}_q^k$ such that $g(x) = \sum_{i=1}^{k} \lambda_i g_i(x)$. Thus, $s(x)$ divides $g(x)$. On the other hand, by Bézout's identity, there exist polynomials $\mu_i(x)$ such that $s(x) = \sum_{i=1}^{k} \mu_i(x) g_i(x)$. As $g(x)$ divides all the $g_i(x)$, it also divides $s(x)$. Therefore $s(x) = g(x)$, and $s(x)$ verifies the claimed properties.

• Now assume the aforementionned properties are satisfied for $s(x)$. Let $\mathcal{C}'$ be the cyclic code generated by $s(x)$. Then the matrix formed by the words corresponding to the $x^i s(x)$ is a generator matrix for $\mathcal{C}'$. Thus, $\mathcal{C}'$ has dimension at least k (i) and is included in $\mathcal{C}$(ii) of dimension k. Therefore $\mathcal{C} = \mathcal{C}'$, which implies that $\mathcal{C}$ is cyclic. □