## 1. Cyclic Codes

**Definition 1.** *A linear code $C \subset \mathbb{F}^n$ over a finite field $\mathbb{F}$ is called a* ***cyclic code*** *if it is a cyclic subset, ie if it is invariant under the cyclic shift $\tau$ defined by*

$$\tau((u_0, u_1, \cdots, u_{n-1})) = (u_{n-1}, u_0, \cdots, u_{n-2}).$$

$\tau$ is obviously a linear map of $\mathbb{F}^n$:

$$\tau(u) = (u_0, u_1, \cdots, u_{n-1})T,$$

where $T$ is the matrix with row $i$ equal to $\tau^i((1, 0, \cdots, 0))$.

Suppose that $u \in \mathbb{F}^n \setminus \{0\}$ and that $k$ is defined as

$$\max\{j > 0 : u, \tau(u), \tau^2(u), \cdots, \tau^{j-1}(u) \text{ is linearly independent}\}.$$

Then $\{u, \tau(u), \tau^2(u), \cdots, \tau^{k-1}(u)\}$ is a basis for a $[n, k]$ cyclic code with generator matrix

$$\begin{bmatrix} u \\ \tau(u) \\ \vdots \\ \tau^{k-1}(u) \end{bmatrix}$$

If $\tau^k(u) = \sum_{i=0}^{k-1} c_i \tau^i(u)$, and $c = vG$ for some $v \in \mathbb{F}^k$ then the cyclic property is reflected in the equalities

$$\tau(c) = cT = vGT = vMG$$

where $M$ is the companion matrix of the polynomial $f(z) = \sum_{i=0}^{k-1} c_i z^i$.

**Example 2.** *Consider the binary code $C$ with generator*

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

*The rows of $G$ are $u$, $\tau(u)$ and $\tau^2(u)$; moreover, $\tau^3(u) = u + \tau^2(u)$. So $C$ is cyclic and*

$$GT = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

As we will see briefly, this construction is in fact completely general. But in order to take advantage of the cyclic structure it is necessary to translate it in a more algebraic form.
Before that, we end this introductory section with a general property that can be proved directly from the definition:

**Proposition 3.** *The dual of a cyclic code is also cyclic.*

*Proof.* **HW**. □

1.1. **Polynomial Representation.** The vector space $\mathbb{F}^n$ may be identified with $\mathbb{F}[x]/(x^n-1)$ through the isomorphism

$$\rho : \mathbb{F}^n \to \mathbb{F}[x]/(x^n-1), \qquad \rho((u_0, u_1, \cdots, u_{n-1})) = \sum_{i=0}^{n-1} u_i x^i;$$

this last space is not only a $\mathbb{F}$-vector space but also a ring, with the usual sum and multiplication of polynomials as operations, which of course are always modulo $x^n-1$. In other words, $\mathbb{F}[x]/(x^n-1)$ is a $\mathbb{F}$-**commutative algebra**. It is obviously not a field (unless $n=1$) because $x^n-1$ is not irreducible. The structure of $\mathbb{F}[x]/(x^n-1)$ will be analysed in greater detail later.

As a consequence of this identification, we consider vectors as polynomials, ie, we identify the vector $u \in \mathbb{F}^n$ with the polynomial $\rho(u)$ or, to be more precise with its equivalence class in the quotient ring.
With this isomorphism, we have the following important interpretation of the cyclic shift, that will be essential from now on:

$$\rho(\tau(u)) = x\rho(u).$$

**Remark 4.** *Because of this identification, when working with cyclic codes, we will index the coordinates of vectors, as well as rows and columns of generator and parity check matrices, starting at* 0 *and not at* 1*, as usual. In this way, the index of a coordinate coincides with the power of* $x$ *of the corresponding term in the polynomial representation.*

**Remark 5.** *Although it is not strictly necessary for the definition, we will always assume that* $n$ *and* $q$ *are coprime where* $N = |\mathbb{F}|$ *is a power of a prime. The case where* $n$ *and* $N$ *ae not co-prime will be discussed later.*

The representation of vectors from $\mathbb{F}^n$ as polynomials adds a richer algebraic structure to that vector space and its subspaces, namely linear codes, as we will now see.
We recall that a subset $S$ of a commutative ring $R$ is a **ideal** if

$$\forall \alpha, \beta \in S \, \forall \gamma \in R : \ \alpha + \beta \in S, \ \gamma\alpha \in S.$$

An ideal $S \subset R$ is **principal** if it is generated by a single element: there exists $\mu \in S$ such that every $\alpha \in S$ is equal to $\gamma\mu$ for some $\gamma \in R$.
Finally, $R$ is said to be a **principal ideal domain** if it does not contain zero divisors and every ideal is principal. Basic examples of principal ideal domains are $\mathbb{Z}$ and $\mathbb{F}[x]$ and in both cases the property is derived from the validity of a Division Lemma and the existence of greatest common divisors.

**Proposition 6.** *All ideals in* $\mathbb{F}[x]/(x^n-1)$ *are principal.*

*Proof.* (**HW**). It is a consequence of the same property for $\mathbb{F}[x]$: given a nonzero ideal $I$ from $\mathbb{F}[x]/(x^n-1)$ and the projection $\pi : \mathbb{F}_q[x] \to \mathbb{F}[x]/(x^n-1)$, consider $\tilde{I} = \pi^{-1}(I)$. □

We now come to an important characterization of cyclic codes:

**Theorem 7.** *A linear code* $C \subset \mathbb{F}[x]/(x^n-1)$ *is cyclic if and only if it is an ideal.*

*Proof.* Suppose $C$ is cyclic. By linearity, given $u(x), v(x) \in C$, $u(x) + v(x) \in C$; to prove the other property , it is enough (**HW**) to prove that for any $u(x) \in C$, $xu(x) \in C$. This was already seen before:

$$xu(x) = x \sum_{i=0}^{n-1} u_i x^i = \sum_{i=0}^{n-1} u_i x^{i+1} = u_{n-1} + u_0 x + \cdots + u_{n-2} x^{n-1}$$

which belongs to $C$ by cyclicity. In the last equality we use of course the fact that $x^n \equiv 1$.
The converse follows the same line of reasoning and is left as an exercise (**HW**). □

As a consequence of the two last results, we have

**Proposition 8.** *If $C \subset F[x]/(x^n - 1)$ is a cyclic code, it contains a unique monic polynomial $g(x)$ of minimal degree, the **generator polynomial** of $C$. This is denoted a $C =< g(x) >$. Moreover, $g(x) \mid (x^n - 1)$ in $\mathbb{F}[x]$ and $k = \dim(C) = n - \deg(g(x))$:*

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

*is a generator matrix for the code.*

*Proof.* (**HW**). □

Conversely,

**Proposition 9.** *If $g(x) \mid (x^n - 1)$ then it is the generating polynomial of a length $n$ cyclic code (with dimension $n - \deg(g(x))$).*

*Proof.* (**HW**): the matrix $G$ defined in the previous proposition is a generator of a linear code $C \subset \mathbb{F}[x]/(x^n - 1)$ and $g(x)$ is the unique polynomial with minimal degree. It remains only to verify that $C$ is cyclic, ie, that $x^k g(x) \in C$. □

**Corollary 10.** *There is a bijection between cyclic codes of length $n$ over $\mathbb{F}$ and monic divisors of $x^n - 1$. If $x^n - 1 = \prod_j p_j^{t_j}$ is the decomposition in irreducible factors, there are $\prod_j (t_j + 1)$ distinct cyclic codes $C \subset \mathbb{F}^n$.*

*Proof.* (**HW**). □

**Example 11.** *$g(x) = x^4 + x^3 + x^2 + 1$ is a divisor of $x^7 - 1$ in $\mathbb{F}_2[x]$ and so is the generator polynomial for a $[7, 3]$-cyclic code over $\mathbb{F}_2$. The corresponding generator matrix is*

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

*We may obviously obtain a different generator, for instance, by Gauss Jordan reduction:*

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

*From either one of them it is easy to confirm that the code has distance $d = 3$ and is a 1 error-correcting code.*

It was noticed before that not every linear code has a generator matrix in standard form. However, for cyclic codes, the existence of a generator in a modified standard form is guaranteed:

**Proposition 12.** *A $[n, k]$ cyclic code has a generator matrix $G = [A\, I_k]$, where $I_k$ denotes the $k$-dimensional identity matrix.*

*Proof.* For every $0 \leq i < k$, we may write $x^{n-k+i} = v_i(x)g(x) + r_i(x)$, where $\deg(r_i(x)) < n - k$. The vectors corresponding to the codewords $x^{n-k+i} - r_i(x)$ constitute a basis of the code with the desired property. (Details are left as **HW**). □

**Exercise 13.** *Find a generator matrix $G = [A \,|\, I_k]$ for the code in the previous example.*

**Remark 14.** *Because the dual of a cyclic code is again cyclic, this implies that a cyclic code has also a generator in standard form.*

1.1.1. *Parity-check matrices and dual codes.* A parity-check matrix for a cyclic code may be obtained from a corresponding generator matrix, as for any linear code. In particular, by the last proposition, we may obtain a parity-check matrix in standard form $H = [I_{n-k} \,|\, B]$.

But it is also possible to derive a parity-check matrix directly from the generator polynomial.
We start by noticing that, if

$$x^n - 1 = g(x)h(x), \qquad g(x) = \sum_{i=0}^{t} g_i x^i, \qquad h(x) = \sum_{j=0}^{n-t} h_j x^j,$$

then

$$\sum_{i=0}^{k} g_i h_{k-i} = 0, \qquad \forall 0 < k < n, ;$$

in particular, for every $t \leq k < n$,

$$\sum_{i=0}^{t} g_i h_{k-i} = 0$$

**Definition 15.** *Given a polynomial $f(x) \in \mathbb{F}[x]$ with degree $m$, its **reciprocal polynomial** is defined as*

$$f_R(x) = x^m f(x^{-1}),$$

*ie, it is the polynomial with the same coefficients in reversed order.*

We show that, given the factorization above and $C$ the code with polynomial generator $g(x)$, $h_R(x) \in C^\perp$: using the basis for $C$ corresponding to

$$g(x), xg(x), \cdots, x^{n-t-1}g(x),$$

this is equivalent (**HW**) to

$$\forall 0 \leq l < n-t,\ \sum_{i=l}^{l+t} g_{i-l}h_{n-t-i} = 0 \Leftrightarrow \forall 0 \leq l < n-t,\ \sum_{i=0}^{t} g_i h_{n-t-l-i} = 0.$$

But these are exactly the equalities obtined above ($k = n-t-l$).
So we obtained

**Proposition 16.** *If $g(x)$ is the generator polynomial of a $[n,k]$-cyclic code $C$ over $\mathbb{F}$ and $x^n - 1 = g(x)h(x)$ then $g^\perp(x) = h(0)^{-1}h_R(x)$, ie, the monic multiple of $h_R(x)$, is the generator for $C^\perp$.*

*Proof.* □

**Exercise 17.** *Find the generator polynomial for $C^\perp$, where $C$ is the code from example 11.*

1.1.2. *Encoding.* Different basis for a cyclic code give rise to different encodings, which may also be interpreted in polynomial form, identifying the source vectors $u = (u_0, \cdots, u_{k-1}) \in \mathbb{F}^k$ with polynomials $u(x) = \sum_{i=0}^{k-1} u_i x^i$.

With the generator matrix associated to the basis

$$g(x), xg(x), \cdots, x^{k-1}g(x),$$

$u(x)$ is encoded to $u(x)g(x)$; this encoding is clearly nonsystematic.

On the other hand, the generator matrix of the form $[A \mid I]$, associated, as we saw above, to the basis

$$x^{n-k} - r_0(x), \cdots, x^{n-1} - r_{k-1}(x),$$

(where the $r_i(x)$ are defined as the remainders of division, in $\mathbb{F}[x]$, of $x^{n-k+i}$ by $g(x)$) gives rise to the systematic encoding

$$u(x) \to x^{n-k}u(x) - r(x)$$

(where, similarly, $r(x)$ is the remainder of the division of $x^{n-k}u(x)$ by $g(x)$).

A second systematic encoding is based not on $G$ but on the corresponding parity-check matrix $H$ obtained from the generator polynomial for $C^\perp$: if the source $u(x)$, with degree less than $k$, is systematically encoded into $c(x) = \sum_{i=}^{n-1} c_i x^i$ then $c_i = u_i$ for $0 \leq i < k$, ie, $c(x) = u(x) + c_k x^k + c_{k+1}x^{k+1} + \cdots + c_{n-1}x^{n-1}$; the equation $Hc^T = 0$ allow us to compute the remaining coefficients $c_i$ iteratively: as the generator polynomial of $C^\perp$, $g^\perp(x) = \sum_{i=0}^{k} t_i x^i$ has degree $k$ (and is monic), the first row of $H$ gives

$$\sum_{i=0}^{k-1} t_i u_i + c_k = 0,$$

the second

$$\sum_{i=1}^{k-1} t_{i-1}u_i + t_{k-1}c_k + c_{k+1} = 0,$$

and so on.

**Example 18.** *Let $C$ be the $[15, 7]$ binary cyclic code with generator polynomial $g(x) = 1 + x^4 + x^6 + x^7 + x^8$. The corresponding generator matrix is*

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

*If the source is $u(x) = 1 + x^2 + x^5$, the encoding using $G$ is*

$$(\ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ )G = (\ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ )$$

*giving $c(x) = 1 + x^2 + x^4 + x^5 + x^7 + x^{10} + x^{11} + x^{12} + x^{13}$, which may be obtained also by polynomial multiplication $c(x) = u(x)g(x)$.*

*Polynomial division gives us*

$$x^8u(x) = g(x)(1 + x + x^4 + x^5) + 1 + x^6$$

*and the first form of systematic encoding described above gives $c(x) = 1 + x^6 + x^8u(x) = 1 + x^6 + x^8 + x^{10} + x^{13}$.*

*The generator polynomial of $C^\perp$ is $g^\perp(x) = 1 + x + x^3 + x^7$ and so we get a parity-check matrix*

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

*Applying the second from of systematic encoding*

$$H(\ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ c_7\ \ c_8\ \ c_9\ \ c_{10}\ \ c_{11}\ \ c_{12}\ \ c_{13}\ \ c_{14}\ ) = 0$$

*gives the message $c(x) = 1 + x^2 + x^5 + x^7 + x^8 + x^{14}$.*

1.2. **Decoding for Cyclic Codes.** We review some general facts about syndrome decoding for linear codes: suppose $C$ is a linear code and that we have fixed an encoding formula, associated with the choice of a generator matrix. If $u$ is a received message, we compute the syndrome $s(u) = uH^T$, where $H$ is a parity-check matrix and, provided that the corresponding coset has a unique coset leader $e$, we decode $u$ as $u - e$.
If $Q$ is an invertible $(n-k)\times(n-k)$ matrix, $QH$ is also a parity-check matrix for $C$; this different choice of parity-check matrix gives rise to different syndromes and/or to a different correspondence between syndromes and cosets, but these, as well as the coset leaders, remain unchanged. Ie, we are free to choose the parity-check matrix for syndrome decoding.
We apply this observvation to the decoding process for cyclic codes:

**Theorem 19.** *If $g(x)$ is the generator polynomial for $C$ and the parity-check matrix has the form $H = [I_{n-k} \mid A]$, then for $u(x) \in \mathbb{F}^n$ $syn(u(x))$ is the remainder of the division of $u(x)$ by $g(x)$; in particular*

$$syn(u(x)) \equiv u(x) \mod g(x).$$

*Proof.* Identifying the columns of $H$ with polynomials, the first $n-k$ columns correspond to $1, x, \cdots, x^{n-k-1}$, while the remaining ones correspond to $a_0(x), \cdots, a_{k-1}(x)$, all of degree less or equal than $n-k-1$.
The matrix $\left[-A^T \mid I_k\right]$ is then a generator for $C$ and so $x^{n-k+i} - a_i(x) \in C$, for all $0 \le i < k$. Let $x^{n-k+i} - a_i(x) = v_i(x)g(x)$; if $u(x) = \sum_{i=0}^{n-1} u_i x^i$, its syndrome is given by

$$S(x) = \sum_{i=0}^{n-k-1} u_i x^i + \sum_{i=0}^{k-1} u_{n-k+i} a_i(x) = \sum_{i=0}^{n-k-1} u_i x^i + \sum_{i=0}^{k-1} u_{n-k+i} \left(x^{n-k+i} - v_i g(x)\right) =$$

$$= u(x) - \left(\sum_{i=0}^{k-1} u_{n-k+i} v_i(x)\right) g(x).$$

As $deg(S(x)) < n-k = deg(g(x))$, we confirm that $S(x)$ is in fact the remainder of the division. □

As we have already noticed in the discussion of encoding, the identification of vectors with polynomials allows the natural embedding of $F^k$ (the space of source vectors which are identified with polynomials of degree less or equal to $k-1$) into $\mathbb{F}^n$. Now, also the syndromes (which belong, for a general linear code, to $\mathbb{F}^{n-k}$) are identified with polynomials of degree less or equal to $n-k-1$ and so with elements of $\mathbb{F}^n$.
This observation, together with the previous theorem, has a useful consequence: suppose that $C$ is $t$-error correcting. This happens if and only if every vector $v$ with $w(v) \le t$ is a coset leader. So, if $w(syn(u)) \le t$, and since $syn(u)$ belongs to the coset containing $u$, we conclude that $syn(u)$ is the error pattern associated to $u$:

**Corollary 20.** *If $C$ is $t$-error correcting and $w(syn(u)) \le t$, then $u$ is decoded into $u - syn(u)$.*

If $w(syn(u)) > t$, to perform syndrome decoding we must find the corresponding coset leader.

**Lemma 21.** *If* $syn(u(x)) = S(x) = \sum_{i=0}^{n-k-1} s_i x^i$, *then* $syn(xu(x)) = xS(x) - s_{n-k-1}g(x)$.

*Proof.* If $u(x) = z(x)g(x) + S(x)$ then

$$xu(x) = xz(x)g(x) + xS(x) = (xz(x) + s_{n-k-1})\, g(x) + (xS(x) - s_{n-k-1}g(x))\,,$$

and $deg\,(xS(x) - s_{n-k-1}g(x)) < n - k$, so this is the remainder of the division of $xu(x)$ by $g(x)$. □

With this observation it is possible to justify a procedure to determine, in certain cases, the coset leader of $u(x)$.
We say that a vector has a **cyclic run** of $l$ zeros if it has $l$ consecutive zeros in the cyclic order.

**Example 22.** *The vector* $(0,0,1,1,0,1,0,0,1,0,0,0,0)$ *has a cyclic run of* 6 *zeros.*

We then have the following decoding procedure, called **error trapping decoding**:

**Proposition 23.** *Let* $C$ *be a* $[n,k,d]$ *cyclic code over* $\mathbb{F}$, *with generator polynomial* $g(x)$.
*Suppose that* $u(x)$ *is a received word. If its error pattern* $e(x) = u(x) - c(x)$ *has weight less or equal than* $t = \lfloor \frac{d-1}{2} \rfloor$ *and a cyclic run of at least* $k$ *zeros, then the following algorithm identifies and corrects it:*

(1) *Compute the syndromes* $S_i(x)$ *of* $x^i u(x)$ *until for some* $m$, $w(S_m(x)) \leq t$;
(2) *compute the remainder* $r(x)$ *of the division of* $x^{n-m}S_m(x)$ *by* $x^n - 1$;
(3) *decode* $u(x)$ *into* $u(x) - r(x)$.

*Proof.* The assumption about the cyclic run of zeros of the error pattern means that there exists an integer $0 \leq m < n$ such that $x^m e(x)$ has all its nonzero coordinates in the first $n - k$ positions, ie, $x^m e(x)$ has degree less or equal than $n - k - 1$; this implies (**HW**) that $x^m e(x) = S_m(x) = syn(x^m u(x))$; since it has, by hypothesis, weight less or equal than $t$, we confirm that, under our assumptions, we will in fact find a $m$ such that $w(S_m(x)) \leq t$.
Now, if $w(S_m(x)) \leq t$, we know that $S_m(x)$ is the coset leader of $x^m u(x)$. Let $x^{n-m}S_m(x) = v(x)(x^n - 1) + r(x)$; as

$$u(x) - r(x) = x^{n-m}(x^m u(x) - S_m(x)) + v(x)(x^n - 1) \equiv 0 \mod g(x),$$

we see that $r(x)$ is in the same coset as $u(x)$, and since $w(r(x)) \leq t$ it must be the coset leader, ie, $r(x) = e(x)$. □

We illustrate the decoding procedure with an example. We leave the computational details as an exercise:

**Example 24.** *We consider a* $[15,7]$ *code* $C$ *over* $\mathbb{F}_2$ *generated by* $g(x) = x^8 + x^7 + x^6 + x^4 + 1$. *As*

$$x^{15} - 1 = g(x)(x^7 + x^6 + x^4 + 1)$$

*we obtain as generator polynomial for the dual code the polynomial* $h_R(x) = 1 + x + x^3 + x^7$. *The check parity matrix for* $C$ *in reduced form is* $H = [I_8 \,|\, A]$ *where*

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

*We see that* $d = 5$, *and so* $C$ *is a* 2 *error correcting code:* 5 *is an obvious upper bound because the minimum weight of the columns of* $A$ *is* 4*; it is then enough to verify that*

- *no linear combination of two columns of* $A$ *has weight less or equal than* 2 *and*
- *no linear combination of three columns of* $A$ *has weight less or equal than* 1.

*We notice that any error pattern with weight less or equal than* 2 *will have a cyclic run of at least* 7 *zeros, which guarantees the success of the algorithm for those error patterns.*
*Suppose the received word is* $(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$, *corresponding to*

$$u(x) = 1 + x + x^4 + x^5 + x^6 + x^8 + x^9 + x^{13};$$

*the list of the first syndromes* $S_i(x)$ *is*

$$\begin{aligned} S_0(x) &= 1 + x^2 + x^5 + x^7 \\ S_1(x) &= 1 + x + x^3 + x^4 + x^7 \\ S_2(x) &= 1 + x + x^2 + x^5 + x^6 + x^7 \\ S_3(x) &= 1 + x + x^2 + x^3 + x^4 \\ S_4(x) &= x + x^2 + x^3 + x^4 + x^5 \\ S_5(x) &= x^2 + x^3 + x^4 + x^5 + x^6 \\ S_6(x) &= x^3 + x^4 + x^5 + x^6 + x^7 \\ S_7(x) &= 1 + x^5 \end{aligned}$$

*We decode* $u(x)$ *as*

$$u(x) - x^8(1+x^5) = u(x) - x^8 - x^{13} = 1 + x + x^4 + x^5 + x^6 + x^9 \;\rightarrow (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0).$$

1.2.1. *Burst error-correcting decoding.* The decoding algorithm described above makes use of a particular property of the error patterns (the existence of a cyclic run of at least $k$ zeros); in certain cases (eg, the previous example), the parameters of the code directly imply that property.

**Exercise 25.** *Determine a condition on the length* $n$, *dimension* $k$ *and minimal distance* $d$ *of a linear code that guarantee that any error pattern with weight less than* $t = \lfloor \frac{d-1}{2} \rfloor$ *has a cyclic run of at least* $k$ *zeros.*

On the other hand, that property is satisfied by error patterns that are concentrated in a relatively short interval of the message. In many practical applications this is a very natural condition to consider. Such a pattern is called a **burst error**:

**Definition 26.** *A burst of length $l > 1$ (or a $l$-burst) is a vector such that the shorter (cyclic) interval containing its nonzero coordinates has length $l$.*
*A code is called $l$-burst-error-correcting if it can correct all bursts of length $l$ or less and $l$-burst-error-detecting if it can detect all bursts of length $l$.*

**Example 27.** 000101010000 *and* 010000000101 *are both bursts of length* 5.

**Remark 28.** *A vector may be seen as a burst in different ways; for example,* 1001100 *has two presentations as a* 5*-burst, starting at different coordinates. However, if $2l < n + 2$, then a vector has at most a presentation as a $l$-burst (**HW**).*

For cyclic codes, a polynomial interpretation is that a $l$-burst is represented by a polynomial $e(x)$ of the form

$$e(x) = x^i b(x) \mod x^n - 1,$$

where $b(x)$ has degree $l - 1$ and $i$ indicates the first coordinate of the burst. As noticed in the previous remark, if $2l < n + 2$ this representation is unique.

**Proposition 29.** *A linear $[n, k, d]$-code $C$ is $l$-burst-error-detecting if $l < d$.*

*Proof.* Obvious... (**HW**). □

Notice that the condition is, in general, only sufficient but not necessary. A sharper bound holds for cyclic codes:

**Theorem 30.** *A $[n, k]$-cyclic code $C$ detects all $l$-bursts if and only if $l \leq n - k$.*

*Proof.* $C$ certainly detects 1-bursts, so we may take $1 < l \leq n - k$. Let $g(x)$ be the generator polynomial for $C$. Assume that the inequality holds; if $v(x)$ is a $l$-burst, then $v(x) = x^i b(x)$ where $0 < deg(b(x)) = l - 1 < n - k$. If $v(x) \in C$ then, because $g(x)$ and $x^i$ are coprime (why?), we must have $g(x) \mid b(x)$ a contradiction.
The bound is sharp because $C$ contains $g(x)$, which is a $n - k + 1$ burst. □

**Theorem 31.** *A linear code $C$ is $l$-burst-error-correcting if and only if each coset contains at most one burst of length $l$ or less.*

*Proof.* **HW** □

**Corollary 32.** *Let $C$ be a $[n, k]$ linear $l$-burst-error-correcting code. Then no nonzero burst of length $2l$ or less is a codeword.*

*Proof.* (**HW**). Hint: consider a possible counterexample $c$ and show that there exists a $u$ such that both $u$ and $c - u$ are bursts of length $\leq l$. □

**Theorem 33** (Reiger bound)**.** *If $C$ is a $[n,k]$ linear code that corrects, using minimal distance decoding, all bursts with length less or equal than $l$, then $2l \leq n-k$.*

*Proof.* Suppose $e$ is a burst of length $2l$ or less; $e$ is the difference of two bursts of length $l$ or less, which must be in different cosets, implying that $e \notin C$.
The proof is completed by the following observation, whose proof is left as an exercise: if a $[n,k]$ code does not contain a burst of length $b$ or less, then $b \leq n-k$. □

**Exercise 34.** *Prove that if a $[n,k]$ code does not contain a burst of length $b$ or less, then $b \leq n-k$.*
***Hint:*** *Consider the set $S$ of vectors whose last $n-b$ coordinates are zero. Justify that they must belong to distinct cosets.*

After these general observations, we return to cyclic codes, which we will verify to be particularly suited to correct burst errors. As a burst of length $l < n-k$ has a cyclic run of more than $k$ zeros, the decoding algorithm presented above may be adapted to the correction of this type of errors, even if the number of errors exceeds $t = \lfloor \frac{d-1}{2} \rfloor$.
We state the corresponding version of the error trapping algorithm, whose proof is similar to the one given above (**HW**):

**Proposition 35.** *Let $C$ be a $[n,k,d]$ cyclic code over $\mathbb{F}$, with generator polynomial $g(x)$ such that bursts of length at most $l$ are contained in distinct cosets ($C$ is $l$-burst error correcting).*
*Suppose that $u(x)$ is a received word. If its error pattern $e(x) = u(x) - c(x)$ is a burst of length at most $l$, then the following algorithm identifies and corrects it:*

1. *Compute the syndromes $S_i(x)$ of $x^i u(x)$ until for some $m$, $(S_m(x))$ is a burst of length at most $l$;*
2. *compute the remainder $r(x)$ of the division of $x^{n-m}S_m(x)$ by $x^n - 1$;*
3. *decode $u(x)$ into $u(x) - r(x)$.*

The details of the following example are left as an exercise (**HW**):

**Example 36.** *The $[15,9,5]$ binary cyclic code with generator polynomial*

$$g(x) = 1 + x + x^2 + x^3 + x^6$$

*is 3-burst-error-correcting. If*

$$r(x) = 1 + x + x^2 + x^4 + x^5 + x^9 + x^{10} + x^{13}$$

*we find that the syndrome of $x^8 r(x)$ is $1 + x + x^2$.*
*This leads to the decoding*

$$r(x) - x^7(1 + x + x^2) = 1 + x + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{13}$$

*Notice that the syndrome of $x^5 r(x)$ is $x^3 + 1$, which is not a burst of lenght less or equal than 3 but has weigth 2. If we chose to correct a random error instead of a burst error, then minimal distance decoding would lead to the decoding*

$$r(x) - x^{10}(1 + x^3) = 1 + x + x^2 + x^4 + x^5 + x^9.$$

1.3. **Zeros and Minimal Distance of a Cyclic Code.** In order to understand the properties of cyclic codes, we analyze their algebraic structure in greater detail. Let $C$ be a $[n,k]$ cyclic code over $\mathbb{F}$ with generator polynomial $g(x)$.
If $\mathbb{F}=\mathbb{F}_q$ (where $q$ is a power of a prime) and $m$ is the order of $q$ modulo $n$, $\mathbb{F}_{q^m}$ contains a primitive $n$-th root of unity $\alpha$; $x^n-1$ has, in this field, the roots

$$\alpha^i,\ 0\leq i<n;$$

as $g(x)$ divides $x^n-1$, it has in $\mathbb{F}_{q^m}[x]$ a factorization

$$g(x)=\prod_{i\in T}(x-\alpha^i),$$

where $T\subset\{0,1,\cdots,n-1\}$ is called the **defining set** of $C$. We have

**Proposition 37.** *The defining set $T$ of a cyclic code satisfies $|T|=n-k$ and is the union of a subset of the cyclotomic cosets modulo $n$ with respect to $q$.*
*If*

$$\{i_1,\cdots,i_l\}$$

*is a system of representatives of the distinct cyclotomic cosets intersecting $T$,*

$$g(x)=\prod_{j=1}^{l}p_{\alpha^{i_j}}(x).$$

*Proof.* (**HW**). □

As a cyclic code $C$ is the ideal of $\mathbb{F}[x]/(x^n-1)$ generated by $g(x)$, it turns out that it may be characterized by $T$:

**Proposition 38.** *For any $c(x)\in\mathbb{F}[x]/(x^n-1)$, $c(x)\in C$ if and only if $c(\alpha^i)=0$ for all $i\in T$.*

*Proof.* (**HW**). □

**Remark 39.** *It must be noticed that the defining set $T$ depends on the choice of the primitive $n$-th root of unity $\alpha$: if $1<l<n$ is prime to $n$, $\alpha^l$ is also a primitive $n$-th root and with respect to it the new defining set is $T'=l^{-1}T=\{il^{-1}$ mod $n:i\in T\}$.*

**Exercise 40.** *Show that if $c(x)$ is a codeword of a cyclic code $C\subset\mathbb{F}_q[x]/(x^n-1)$, then its zero set $Z(c)=\{i:c(\alpha^i)=0\}$ is a union of cyclotomic cosets modulo $n$, with respect to $q$.*

We discuss now the problem of estimating the distance $d$ of cyclic codes. We prove the simplest general bound for this class of codes, the BCH bound:

**Theorem 41.** *Suppose that $C$ is a $[n,k,d]$ cyclic code over $\mathbb{F}_q$, with generator polynomial $g(x)$, and $\alpha$ is a primitive $n$-th root of unity in $\mathbb{F}_{q^m}$ where $m$ is the order of $q$ modulo $n$. Let $T$ be the defining set of $C$ with respect to $\alpha$, ie,*

$$T=\{0\leq i\leq n:g(\alpha^i)=0\}.$$

*If $T$ contains $\delta$ cyclically consecutive elements, then $d\geq\delta+1$.*

*Proof.* By assumption the zeros of $C$ include $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-1}$. Let $c(x) = \sum_{i=0}^{n-1} c_i x^i$ be a codeword of minimal weight $d$ and let $c = (c_{i_0}, c_{i_1}, \cdots, c_{i_{d-1}})^t$ be the column vector whose coordinates are all the nonzero coefficients. Suppose that $d < \delta + 1$; then the matrix

$$M = \left[\alpha^{(b+s)i_j}\right]_{0 \le s < d}^{0 \le j < d},$$

where $s$ is the row index and $j$ the column index, satisfies $Mc = 0$.
But

$$\det(M) = \alpha^{b(i_0+\cdots+i_{d-1})} \det\left[\alpha^{si_j}\right]_{0 \le s < d}^{0 \le j < d}$$

and this last matrix is a Vandermonde matrix with a nonzero determinant, a contradiction. □

**Remark 42.** *Vandermonde matrices will be used when studying a particular class of codes (Reed-Solomon codes), and their properties will be discussed at that point.*

**Remark 43.** *The application of this result depends on the choice of $\alpha$. As noticed before, replacing $\alpha$ with $\alpha^l$, for some $l$ prime to $n$, the defining set $T$ is replaced with $l^{-1}T$, which may contain a longer sequence of consecutive elements.*

**Example 44.** *We consider again the $[15, 7]$ cyclic code which has generator*

$$g(x) = x^8 + x^7 + x^6 + x^4 + 1$$

*and confirm that it has in fact minimal distance 5. We start by computing the cyclotomic cosets modulo 15, with respect to 2:*

$$C_0 = (0), C_1 = (1, 2, 4, 8), C_2 = (3, 6, 12, 9), C_3 = (7, 14, 13, 11), C_4 = (5, 10).$$

*Eeach coset $C_i$ corresponds to an irreducible factor $p_i(x)$ of $x^{15} - 1$. So $g(x)$ is the product of two of the degree 4 factors, and the BCH bound guarantees that for two of these products, $p_1p_2$ and $p_2p_3$, the minimal distance of the code generated by them is at least 5, as the union of the corresponding cosets contains 4 cyclically consecutive elements.*
*It is easy to compute the polynomials $p_i(x)$ because they are the only degree 4 irreducible polynomial over $\mathbb{F}_2$: they must satisfy $p(0) = p(1) = 1$ and we need to exclude $x^4 + x^2 + 1 = (x^2 + x + 1)^2$, where $x^2 + x + 1$ is the unique irreducible degree 2 polynomial; so the $p_i$ are (in some order)*

$$x^4 + x + 1, \qquad x^4 + x^3 + 1, \qquad x^4 + x^3 + x^2 + x + 1.$$

*Moreover, two of the polynomials have, in $\mathbb{F}_{2^4}$, primitive elements as roots: we know the order of the roots of each irreducible polynomial, in the corresponding splitting field, is the same, and $\mathbb{F}_{2^4}$ has $\phi(15) = 8$ primitive elements. This implies that the order of the roots of one of the polynomials must be 5, corresponding to the coset $C_2$, and we verify that it is the last one: if $\beta$ is a root*

$$\beta^5 = \beta^4 + \beta^3 + \beta^2 + \beta = 1.$$

*We may choose either of the remaining two degree 4 polynomials to define a primitive element (notice that the correspondance between the two polynomials and the cosets $C_1$ and $C_3$ depends on the choice of the primitive root). But in this case*

*we don't even need to work with the primitive element; to confirm that $g(x)$ corresponds to one of the two desired products, we just need to verify that $p_2(x) = x^4 + x^3 + x^2 + x + 1$ divides $g(x)$.*
*Alternatively, we could see that the remaining product*

$$p_1(x)p_3(x) = (x^4 + x + 1)(x^4 + x^3 + 1)$$

*does not coincide with $g(x)$.*

**Example 45.** *In this example we determine a $[13, 5]$ cyclic code over $\mathbb{F}_5$. We start by noticing that the order of 5 modulo 13 is 4, and so $x^{13} - 1$ splits completely in $\mathbb{F}_{5^4}$. The cyclotomic cosets modulo 13 with respect to 5 are*

$$C_0 = (0), \qquad C_1 = (1, 5, 12, 8), \qquad C_2 = (2, 10, 11, 3), \qquad C_3 = (4, 7, 9, 6),$$

*and we have, given a primitive 13-root of identity $\alpha$, the corresponding irreducible polynomials $p_i(x) = \prod_{j\in C_i}(x - \alpha^j)$.*
*$C_1 \cup C_3$ contain a sequence of 6 consecutive elements and so there exists a degree 8 generator polynomial $g(x)$ with 6 roots, implying that the minimal distance of the code will be at least 7. In fact, any product of two degree 4 factors $p_i(x)$ will satisfy this condition: this is because $\alpha^j$ has order 13 for any $j \in \{1, \cdots, 12\}$; so, for an appropriate choice of primitive $n$-root of identity $\lambda = \alpha^t$, any product of two degree 4 factors $p_i(x)$ will equal $\prod_{j\in C_1\cup C_3}(x - \lambda^j)$.*
*The difficulty lies in determining the polynomials $p_i(x)$, as we don't know in advance a primitive 13-root of identity $\alpha$. We would need to identify, from the 150 degree 4 irreducible polynomials over $\mathbb{F}_5$ the three that have order 13.The most common solution for this type of problem is either to look for the answer in available lists of irreducible polynomials or to use a computer. It is possible, however, to solve the problem directly and the ideas involved may even be helpful in more general settings. The details of the computations are left as an exercise.*
*We fix the unknown 13-root $\alpha$ and write the polynomials as sums of monomials: for $p_1(x)$ we obtain*

$$p_1(x) = (x - \alpha)(x - \alpha^5)(x - \alpha^8)(x - \alpha^{12}) =$$

$$= x^4 - (\alpha + \alpha^5 + \alpha^8 + \alpha^{12})x^3 + (2 + \alpha^4 + \alpha^6 + \alpha^7 + \alpha^9)x^2 - (\alpha + \alpha^5 + \alpha^8 + \alpha^{12})x + 1.$$

*This expression leads us naturally to consider the sums $a_i = \sum_{j\in C_i} \alpha^j$; the expression above becomes*

$$p_1(x) = x^4 - a_1x^3 + (2 + a_3)x^2 - a_1x + 1,$$

*and we find in a similar way, that*

$$p_2(x) = x^4 - a_2x^3 + (2 + a_1)x^2 - a_2x + 1, \qquad [p_3(x) = x^4 - a_3x^3 + (2 + a_2)x^2 - a_3x + 1.$$

*We know that*

$$p_1(x)p_2(x)p_3(x) = \sum_{i=0}^{12} x^i,$$

*and comparing coefficients for $i < 4$, we deduce (**HW**) the relations*

$$\begin{cases} a_1 + a_2 + a_3 = -1 \\ a_1a_2 + a_1a_3 + a_2a_3 = 1 \\ a_1a_2a_3 = -1 \end{cases}$$

*These symmetric polynomials on the $a_i$ appear in the well known Newton relations:*
$(y-a_1)(y-a_2)(y-a_3) = y^3-(a_1+a_2+a_3)x^2+(a_1a_2+a_1a_3+a_2a_3)x-a_1a_2a_3 = y^3+y^2+y+1.$
*But the roots of this last polynomial in $\mathbb{F}_5$ are 2, 3 and 4 (why?) and so we determined the $a_i$. However the relations obtained are not enough: for instance, assuming (with no loss of generality) that $a_1 = 2$, is $a_3$ equal to 3 or to 4? In the first case, we would have*

$$p_1(x) = x^4 + 3x^3 + 3x + 1$$

*while in the second*

$$p_1(x) = x^4 + 3x^3 + x^2 + 3x + 1.$$

*Either by computing the order of the polynomials or by identifying which one is a factor of $x^{13} - 1$, we find that the first is the correct option.*
*We may finally write explicitly the polynomials $p_i(x)$:*

$$x^4 + 3x^3 + 3x + 1, \qquad x^4 + x^3 + 4x^2 + x + 1, \qquad x^4 + 2x^3 + x^2 + 2x + 1.$$

**Example 46.** *Suppose we want to construct a binary cyclic code of length 11. We may start with the observation that the two factors in the polynomial decomposition $x^{11} - 1 = (x - 1)\sum_{j=0}^{10} x^j$ are irreducible over $\mathbb{F}_2$. In fact, let $f(x) = \sum_{j=0}^{10} x^j$; the irreducibility of $f(x)$ may be confirmed by Rabin's criterion: the conditions*

$$f(x) \mid (x^{2^{10}} - x), \qquad \gcd(f(x), x^{2^5} - x) = \gcd(f(x), x^{2^2} - x) = 1$$

*are easily verified, even by hand. We could also confirm these conditions noticing that $2^{10} - 1 = 3 \times 11 \times 31$ and in $\mathbb{F}_{2^{10}}$*

- *$f(x)$ splits completely as the product of factors $(x-\lambda)$ where $\lambda$ is a primitive 11-root of 1,*
- *$x^{2^5} - x$ splits as $x(x-1)\prod(x-\lambda)$, with $\lambda$ a primitive 31-root of 1,*
- *and $x^{2^2} - x$ splits as $x(x-1)\prod(x-\lambda)$, with $\lambda$ a primitive 3-root of 1.*

*This shows that the only non-trivial binary cyclic codes of length 11 have dimension 1 or 11.*
*However, we have other cyclic codes by passing to an extension field: as we know, $f(x)$ factors as the product of two degree 5 irreducible polynomials $p_1(x)$ and $p_2(x)$ over $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ (where $\alpha^2 = \alpha + 1$). Concretely, let $\beta$ denote a primitive 11-root of unity (in $\mathbb{F}_{2^{10}}$); as the cyclotomic cosets modulo 11 with respect to 4 are*

$$C_0 = (0), \quad C_1 = (1, 4, 5, 9, 3), \qquad C_2 = (2, 8, 10, 7, 6),$$

*we have $p_i(x) = \prod_{j\in C_i}(x - \beta^j)$. Expanding these products, one finds that, putting $a = \sum_{j\in C_1} \beta^j$ and $b = \sum_{j\in C_2} \beta^j$,*

$$p_1(x) = x^5 + ax^4 + x^3 + x^2 + bx + 1, \qquad p_2(x) = x^5 + bx^4 + x^3 + x^2 + ax + 1;$$

*as neither $a$ or $b$ is in $\mathbb{F}_2$ and $a + b = 1$, we know that we may take $a = \alpha$ and $b = \alpha^2$.*
*If we choose, for instance, $(x - 1)p_1(x)$ as the generator polynomial, we obtain a $[11, 5, d]$ code over $\mathbb{F}_4$ with $d \geq 4$.*

*By a (very) tiresome verification or applying more advanced results, we find that $d = 5$ and so the code is 2-error correcting. Moreover, any error pattern with weight 2 contains a string of cyclically consecutive zeros with length at least 5, and so the error-trapping algorithm may be applied.*

**Exercise 47.** *Show that the code from the last example is not* 3*-burst error correcting.*

1.3.1. *Generating Polynomials and Idempotents.* Besides the generator polynomial $g(x)$, other polynomials also generate the same ideal, ie, the same code:

**Proposition 48.** *$v(x) \in \mathbb{F}[x]/(x^n-1)$ generates $C$ if and only if, in $\mathbb{F}[x]$,*

$$gcd(v(x), x^n - 1) = g(x).$$

*Proof.* Suppose that $gcd(v(x), x^n - 1) = g(x)$. This implies that $v(x) \in < g(x) > = C$; on the other hand, there exist $a(x), b(x) \in \mathbb{F}[x]$ such that

$$g(x) = a(x)v(x) + b(x)(x^n - 1),$$

implying that, modulo $x^n - 1$, $g(x) = a(x)v(x)$ and so the ideal generated by $g(x)$ is contained in the ideal of $\mathbb{F}[x]/(x^n - 1)$ generated by $v(x)$.
For the converse, assume $C =< v(x) >$; then, because $g(x) \in C$, there must exist polynomials $a(x), b(x) \in \mathbb{F}[x]$ such that

$$g(x) = a(x)v(x) + b(x)(x^n - 1);$$

if $d(x) = gcd(v(x), x^n - 1)$, this implies that $d(x) \mid g(x)$; but $d(x)$, by a reasoning similar to the above also belongs to $C$; as $g(x)$ is the unique monic polynomial with minimal degree contained in $C$, we must have $g(x) = d(x)$. □

The proof shows that the generator polynomial is obtained as a greatest common divisor:

**Proposition 49.** *If $C \subset \mathbb{F}[x]/(x^n - 1)$ is a cyclic code generated by a polynomial $v(x)$, the generator polynomial $g(x)$ of $C$ is the greatest common divisor of $v(x)$ and $x^n - 1$ in $\mathbb{F}[x]$.*

*Proof.* Let $d(x) = \gcd(v(x), x^n - 1)$. Because

$$v(x) = a(x)g(x) + f(x)(x^n - 1) = [a(x) + f(x)h(x)]g(x),$$

$g(x)$ divides $d(x)$. But also

$$g(x) = v(x)u(x) + (x^n - 1)$$

and so $d(x)$ must divide $g(x)$. □

**Definition 50.** *A polynomial $e(x) \in \mathbb{F}[x]/(x^n-1)$ is an **idempotent** if $e(x)e(x) = e(x)$ (more precisely, if this equality holds modulo $x^n - 1$).*

It turns out that each cyclic code $C \subset \mathbb{F}[x]/(x^n-1)$ contains - and is determined by - a unique generating idempotent:

**Proposition 51.** *Given a cyclic code $C \subset \mathbb{F}[x]/(x^n - 1)$,*

i) *a nonzero idempotent $e(x) \in C$ generates the code if and only it is a unit of $C$, ie for all $c(x) \in C$, $e(x)c(x) = c(x)$;*
ii) *there exists a unique idempotent $e(x)$ such that $C =< e(x) >$.*

*Proof.* To prove i) we notice that, if $e(x)$ is a nonzero idempotent and a unit of $C$, then, for any $c(x) \in C$, $c(x) = c(x)e(x) \in < e(x) >$, and so $e(x)$ generates $C$. Conversely, if $0 \neq e(x)$ is an idempotent and $C =< e(x) >$, then any $c(x) \in C$ is of the form $c(x) = f(x)e(x)$, but

$$e(x)c(x) = e(x)e(x)f(x) = e(x)f(x) = c(x),$$

ie, $e(x)$ is a unit in $C$.
Since $n$ is prime to the order $q$ of the field $\mathbb{F}$, $x^n - 1$ has no multiple roots in its splitting field over $\mathbb{F}$, and so the Euclidean algorithm for $\mathbb{F}[x]$ implies the existence of polynomials $a(x)$ and $b(x)$ such that

$$1 = a(x)g(x) + b(x)h(x)$$

where $h(x) = \frac{x^n-1}{g(x)}$.
Define $e(x) = a(x)g(x)$ (modulo $x^n - 1$); obviously $e(x) \in C$, and

$$e(x)e(x) = a(x)g(x)\,(1 - b(x)h(x)) = a(x)g(x) - a(x)b(x)(x^n - 1) \equiv e(x) \mod x^n - 1.$$

Uniquenes follows from i): if $e(x)$ and $e'(x)$ are two idempotents that generate $C$, they are both units in $C$ and so

$$e(x) = e(x)e'(x) = e'(x).$$

□

**Example 52.** *Let $C \subset \mathbb{F}_3[x]/(x^{11} - 1)$ be the cyclic code with generator polynomial*

$$g(x) = x^5 + x^4 + 2x^3 + x^2 + 2;$$

*then $h(x) = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1$ and applying the Euclidean algorithm*

$$1 = (x^4 + x^3 + 1)h(x) + (2x^5 + x^4 + x^2)g(x).$$

*So the generating idempotent of $C$ is $e(x) = 2(x^{10} + x^8 + x^7 + x^6 + x^2)$.*

**Proposition 53.** *Let $C_1$ and $C_2$ be cyclic codes of length $n$ over the same field $\mathbb{F}$ with generator polynomials $g_i(x)$ and generating idempotents $e_i(x)$ ($i \in \{1, 2\}$). Then $C_1 \cap C_2$ and $C_1 + C_2$ are both cyclic codes and*

i) *$C_1 \cap C_2$ has generator $\operatorname{lcm}(g_1(x), g_2(x))$ and generating idempotent $e_1(x)e_2(x)$,*
ii) *$C_1 + C_2$ has generator $\gcd(g_1(x), g_2(x))$ and generating idempotent $e_1(x) + e_2(x) - e_1(x)e_2(x)$.*

*Proof.* (**HW**) □

The generating idempotents are helpfull in the construction of certain families of cyclic codes and in the study of their properties. For now, we see how they are related to the algebraic structure of the algebras $\mathbb{F}[x]/(x^n - 1)$ anf its ideals (ie, cyclic codes).

**Remark 54.** *The results that follow are in fact particular cases of the Wedderburn Structure Theorems for semi-simple commutative algebras.*

We have in $\mathbb{F}[x]$ the factorization $x^n - 1 = \prod_{i \in I} f_i(x)$ in distinct irreducible factors. We denote by $\hat{f}_i(x) = \frac{x^n-1}{f_i(x)}$.

**Theorem 55.** *Given the factorization $x^n - 1 = \prod_{i \in I} f_i(x)$,*

i) *the ideals* $< \hat{f}_i(x) >$ *are all the minimal nonzero ideals of* $\mathbb{F}[x]/(x^n-1)$*;*
ii) *we have the following direct sum decomposition* $\mathbb{F}[x]/(x^n-1) = \oplus_i < \hat{f}_i(x) >$*;*
iii) *the generating idempotents* $\hat{e}_i(x)$ *of* $< \hat{f}_i(x) >$ *satisfy* $\hat{e}_i(x)\hat{e}_j(x) = 0$ *for all* $i \neq j$*;*
iv) $\sum_{i\in I} \hat{e}_i(x) = 1$*;*
v) *the only idempotents of* $< \hat{f}_i(x) >$ *are* $0$ *and* $\hat{e}_i(x)$*;*
vi) *If* $e(x)$ *is a nonzero idempotent there is a subset* $J \subset I$ *such that*

$$e(x) = \sum_{i\in J} \hat{e}_i(x) \qquad < e(x) >= \oplus_{i\in J} < \hat{f}_i(x) > .$$

**Proposition 56.** *The minimal ideals of* $\mathbb{F}[x]/(x^n-1)$ *are extension fields of* $\mathbb{F}$*: the map*

$$\mathbb{F}[x]/(f_i(x)) \to < \hat{f}_i(x) >, \qquad v(x) \to v(x)\hat{e}_i(x)$$

*is a ring isomorphism.*

The proof of both results is left as a possible exercise (**HW**), but we illustrate them with a simple example:

**Example 57.** *Let* $q = 2$ *and* $n = 7$*. Over* $\mathbb{F}_2$ *we have the irreducible factorization*

$$x^7 - 1 = f_0(x)f_1(x)f_2(x)$$

*with*

$$f_0(x) = x + 1, \qquad f_1(x) = x^3 + x + 1, \qquad f_2(x) = x^3 + x^2 + 1.$$

*The corresponding* $\hat{f}_i(x)$ *and* $\hat{e}_i(x)$ *are*

$$\begin{cases} \hat{f}_0(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = \hat{e}_0(x) \\ \\ \hat{f}_1(x) = x^4 + x^3 + x^2 + 1, \ \hat{e}_1(x) = x^6 + x^5 + x^3 + 1 \\ \\ \hat{f}_2(x) = x^4 + x^2 + x + 1 = \hat{e}_2(x) \end{cases}$$

*Obviously* $\mathbb{F}_2[x]/(x+1) = \mathbb{F}_2$*. Denoting*

$$\mathbb{F}_2[x]/(f_1(x)) = \mathbb{F}_2[\alpha] \qquad \mathbb{F}_2[x]/(f_2(x)) = \mathbb{F}_2[\beta]$$

*we have the direct sum decomposition*

$$\mathbb{F}_2[x]/(x^7-1) \simeq \mathbb{F}_2 \oplus \mathbb{F}_2[\alpha] \oplus \mathbb{F}_2[\beta].$$

*This isomorphism sends* $v(x)$ *to* $(v(1), v(\alpha), v(\beta))$*.*

## 1.4. **Supplementary Results and Problems.**

**Exercise 58.** *Find a generator polynomial and a generator matrix for a* $[15, 5, d]$ *binary cyclic code that corrects all errors with weight less or equal than* $3$*.*

**Exercise 59.**
a) *Determine all the possible dimensions of cyclic codes of length* $13$ *over* $\mathbb{F}_3$*.*
b) *Verify that* $p(x) = x^3 + 2x + 1$ *is irreducible over* $\mathbb{F}_3$ *and use it to determine a primitive* $13$*-th root of unity.*

c) *Use the previous results to justify that* $g(x) = x^7 + 2x^6 + x^5 + 2x^4 + x^2 + 2$ *is the generator polynomial of a* $[13, 6, d]$ *cyclic code with* $d \geq 5$.
d) *Encode by some form of systematic encoding the source message* $(0, 1, 1, 2, 0, 1)$.
e) *Decode by error trapping the received word*

$$r = (1, 0, 1, 1, 2, 1, 0, 1, 2, 0, 1, 2, 2),$$

*assuming the error has weight less or equal than* 2.
f) *Find if the code corrects all bursts with weight* 3.

**Exercise 60.** *Let* $C$ *be the binary* $[15, 9]$ *cyclic code with generator polynomial*

$$g(x) = 1 + x^3 + x^4 + x^5 + x^6.$$

$C$ *is known to be a* 3*-burst error correcting code.*
*Decode* $(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$.

**Exercise 61.** *Determine the smallest length of a binary cyclic code with generator polynomial*

$$g(x) = 1 + x^4 + x^5.$$

**Exercise 62.** *Let* $C$ *be a cyclic code over* $\mathbb{F}_q$ *with defining set* $T$ *and generator polynomial* $g(x)$. *Let* $C_e$ *be the subcode*

$$C_e = \{c = (c_i) \in C : \sum_i c_i = 0\}.$$

a) *Prove that* $C_e$ *is cyclic and has defining set* $T \cup \{0\}$.
b) *Prove that* $C = C_e$ *if and only if* $0 \in T$ *if and only if* $g(1) = 0$.
c) *Prove that if* $C \neq C_e$ *then the generator polynomial of* $C_e$ *is* $(x - 1)g(x)$.