0.1 Definition

Cyclic codes form an important type of codes for several theoritical as well as practical reasons. From theoritical perspective, they can be expressed as a rich algebraic structure, while practically they can be efficiently implemented. Furthermore, various important codes such as binary Hamming codes and BCH codes, are equivalent to cyclic codes.

Definition 0.1. A code C is ***cyclic*** if(i) C is a linear code; and (ii) any cyclic shift of a codeword is also a codeword, i.e. whenever $a_0 a_1 \cdots a_{n-1}$ is in C, then so is $a_{n-1} a_0 a_1 \cdots a_{n-2}$.

Example:
The linear code $\{0000,\ 1001,\ 0110,\ 1111\}$ is not cyclic, but it is *equivalent* to a cyclic code; interchanging the third and fourth coordinates gives the cyclic code $\{0000,\ 1010,\ 0101,\ 1111\}$.

When considering cyclic codes we number the coordinate positions $0, 1, \ldots, n-1$. This is because then a vector $a_0 a_1 \cdots a_{n-1}$ in $V(n, q)$ correspond to the polynomial $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$.

0.2 Polynomials over finite fields

We denote by $F[x]$ the set of polynomials in x with coefficients in F_q (or simply F with q understood).

Degree of a polynomial in $F[x]$ is defined as usual. These polynomials can be added, subtracted and multiplied in the usual way, thus forming the algebraic structure, *ring*, not a field as they do not have multiplicative inverses.
Division algorithm states the same as in with the polynomials over $\mathbb{R}$, i.e. for every pair of polynomials $a(x)$ and $b(x) \neq 0$ in $F[x]$, there exists a unique polynomials $q(x)$, and $r(x)$, such that

$$a(x) = q(x)b(x) + r(x),$$

where deg $r(x) <$ deg $b(x)$.

Now we will establish similarites between the ring $F[x]$ of polynomials and the ring $\mathbb{Z}$ of integers. Just as the ring $\mathbb{Z}_m$ is obtained after modulo m, we can consider polynomials in $F[x]$ modulo some $f(x)$. It is natural to define $g(x)$ and $h(x)$ as *congruent modulo* $f(x)$, symbolized by

$$g(x) \equiv h(x) \pmod{f(x)}$$

if $g(x) - h(x)$ is divisible by $f(x)$.

We denote by $F[x]/f(x)$ the set of polynomials in $F[x]$ of degree less than deg $f(x)$, with addition defined as normal addition as adding two polynomials in $F[x]/f(x)$ will not increase the degree; while multiplication is defined congruent modulo $f(x)$, i.e for any two polynomials in $F[x]/f(x)$, a unique polynomial of degree less than deg $f(x)$.

Finally, the set $F[x]/f(x)$ is called a *ring of polynomials(over F) modulo* $f(x)$ and it is quite obvious that

$$|F_q[x]/f(x)| = q^n.$$

Now the next logical step is to find out when this ring forms a field, i.e. when each of the polynomials in $F[x]/f(x)$ have a multiplicative inverse.
For that we will first define *reducibility* of polynomials.

Definition 0.2. A polynomial $f(x)$ is called ***reducible*** if $f(x) = a(x)b(x)$, where $a(x), b(x) \in F[x]$ and deg $a(x)$, deg $b(x)$ are both smaller than deg $f(x)$. If $f(x)$ is not *reducible*, it is called ***irreducible***.

Theorem 0.3. The ring $F[x]/f(x)$ is a field if and only if $f(x)$ is irreducible in $F[x]$.

Proof. The proof follows the same line as followed by the proof of Theorem **??**, with prime m being replaced by $f(x)$. □

0.3 Cyclic codes expressed as polynomials

From now on, we will fix $f(x) = x^n - 1$, as the ring $F[x]/(x^n - 1)$ of the polynomials modulo $x^n - 1$ is the natural one to consider in the context of cyclic codes. We will now denote $F[x]/(x^n - 1)$ as R_n, where the field $F = F_q$ will be understood.
Since $x^n \equiv 1 \pmod{x^n - 1}$, we can reduce any polynomial modulo $x^n - 1$ simply by replacing x^k by $x^{k \pmod{n}}$, without any long division.

We will now denote a vector $a_0 a_1 \cdots a_{n-1}$ in $V(n, q)$ with the polynomial

$$a(x) = a_0 + a_1 x + \cdots + a^{n-1} x^{n-1}$$

in R_n, that is, now a code C is subset of both $V(n, q)$ and R_n. Note that addition of vectors and multiplication of a vector by a scalar in R_n corresponds exactly to those operations in $V(n, q)$.
Now, it must be clear that *multiplying* by x^m to $a(x)$ corresponds to a cyclic shift through m positions. We can model cyclic codes in a way, given by the following theorem.

Theorem 0.4. A code C in R_n is a cyclic code if and only if C satisfies the following two conditions:

(i) $a(x), b(x) \in C \implies a(x) + b(x) \in C$,

(ii) $a(x) \in C$ and $r(x) \in R_n \implies r(x)a(x) \in C$.

Proof. Suppose C is a cyclic code in R_n. Then C is linear and so (i) holds. Now suppose $a(x) \in C$ and $r(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} \in R_n$. Since, $x^m a(x) \in C \forall m$ (cyclic shifts). Hence,

$$r(x)a(x) = r_0 a(x) + r_1 x a(x) + \cdots + r_{n-1} x^{n-1} a(x)$$

is also in C since each summand is in C. Thus, (ii) also holds.
Now suppose (i) and (ii) hold. Taking $r(x)$ as a scalar, the conditions imply that C is linear. Taking $r(x) = x$ in (ii) shows that C is cyclic. ☐

Now we have a easy way of constructing cyclic codes. Let $f(x)$ be any polynomial in R_n, then we define

$$\langle f(x) \rangle = \{ r(x) f(x) | r(x) \in R_n \}$$

$\langle f(x) \rangle$ is a cyclic code for all $f(x)$ in R_n, as it satisfies the conditions of Theorem 0.4.

Theorem 0.5. Let C be a non-zero cyclic code in R_n. Then

(i) there exists a unique monic (coefficient of highest degree term 1) polynomial $g(x)$ of smallest degree in C,

(ii) $C = \langle g(x) \rangle$,

(iii) $g(x)$ is a factor of $x^n - 1$.

Proof. (i) Suppose $g(x)$ and $h(x)$ are both monic polynomials in C of the smallest degree. Then $g(x) - h(x) \in C$ and has smaller degree. This gives a contradiction if $g(x) \neq h(x)$, for then a suitable scalar multiple of $g(x) - h(x)$ is monic.
(ii) Suppose $a(x) \in C$. By the division algorithm for $F[x]$, $a(x) = q(x)g(x) + r(x)$, where deg $r(x) <$ deg $g(x)$. But $r(x)$, belongs to C, as C is linear. By minimality of deg $g(x)$, we must have $r(x) = 0$ and so $a(x) \in \langle g(x) \rangle$.
(iii) Again by division algorithm, $x^n - 1 = q(x)g(x) + r(x)$ where deg $r(x) < g(x)$. But then $r(x) \equiv -q(x)g(x) \pmod{x^n - 1}$, and so $r(x) \in \langle g(x) \rangle$. By minimality again, $r(x) = 0$, which implies $g(x)$ is a factor of $x^n - 1$. ☐

Definition 0.6. In a non-zero cyclic code C the monic polynomial of least degree, given by theorem 0.5, is called the ***generator polynomial*** of C.

The third part of Theorem 0.5 gives us method of finding all the cyclic codes of length n. All we need are the factors of $x^n - 1$.

Example:
Finding all the binary cyclic codes of length 3. We have $x^3 - 1 = (x+1)(x^2 + x + 1)$, where $x + 1$ and $x^2 + x + 1$ are irreducible over $GF(2)$. So the codes are

Generator ploynomial	Code in R_3	Corresponding code in $V(3,2)$
1	all of R_3	all of $V(3,2)$
$x+1$	$\{0, 1+x, x+x^2, 1+x^2\}$	$\{000, 110, 011, 101\}$
x^2+x+1	$\{0, 1+x+x^2\}$	$\{000, 111\}$
$x^3-1=0$	$\{0\}$	$\{000\}$

Lemma 0.7. Let $g(x) = g_0 + g_1x + \cdots + g_rx^r$ be the generator polynomial of a cyclic code, then g_0 is non-zero.

Proof. Suppose $g_0 = 0$. Then $x^{n-1}g(x) = x^{-1}g(x)$ is a codeword of C of degree $r-1$, contradicting the minimality of deg $g(x)$. □

Now, we are going to define generator matrix (thus, dimensions of C) directly from generator polynomial.

Theorem 0.8. Suppose C is a cyclic code with generator polynomial

$$g(x) = g_0 + g_1x + \cdots + g_rx^r$$

of degree r. Then dim $(C) = n - r$ and a generator matrix C is

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & & g_r & & \vdots \\ \vdots & \vdots & & \ddots & \ddots & \ddots & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & & g_r \end{bmatrix}$$

Proof. The $n-r$ rows of the above matrix G are certainly linearly independent due echelon of non-zero g_0s. The $n-r$ rows represent the cyclic permutations of codeword $g(x)$. The proof of Theorem 0.5(ii) shows that if $a(x)$ is a codeword of C, then

$$a(x) = q(x)g(x)$$

for some polynomial $q(x)$, and that this is an equality of polynomials within $F[x]$, i.e. without any modulo. Since deg $a(x) < n$, it follows that deg $q(x) < n - r$. Hence,

$$\begin{aligned} q(x)g(x) &= (q_0 + q_1x + \cdots + q_{n-r-1}x^{n-r-1})g(x) \\ &= q_0g(x) + q_1xg(x) + \cdots + q_{n-r-1}x^{n-r-1}g(x), \end{aligned}$$

which shows that every codeword can be written as a linear combination of those $n-r$ rows. □

Definition 0.9. Let C be a cyclic $[n,k]$-code with generator polynomial $g(x)$. By Theorem 0.5 $g(x)$ is a factor of $x^n - 1$ and so

$$x^n - 1 = g(x)h(x),$$

for some polynomial $h(x)$. $h(x)$ is of degree k, and is called the ***check-polynomial*** of C.

Theorem 0.10. Suppose C is a cyclic code in R_n with generator polynomial $g(x)$ and check polynomial $h(x)$. Then $c(x) \in R_n$ is a codeword in C if and only if $c(x)h(x) = 0$.

Proof. The forward implication is trivial as $g(x)h(x) = 0$. On the other hand, suppose $c(x)$ satisfies $c(x)h(x) = 0$. If $r(x)$ is the remainder of $c(x)$ with $g(x)$ then $r(x)h(x) = 0 \pmod{x^n - 1}$. But deg $(r(x)h(x)) < n - k + k = n$, so $r(x) = 0$, then $c(x) = q(x)g(x) \in C$. □

Theorem 0.11. Suppose C is a cyclic $[n,k]$-code with check polynomial

$$h(x) = h_0 + h_1x + \cdots + h_kx^k$$

Then a parity check matrix for C is

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ & & \ddots & \ddots & & \ddots & & 0 \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & & h_0 \end{bmatrix}$$

Proof. By Theorem 0.10, $c(x)$= $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ is codeword if and only if $c(x)h(x) = 0$. Thus any codeword $c_0c_1 \cdots c_{n-1}$ of C is orthogonal to the vector $h_kh_{k-1} \cdots h_0 \cdots 0$ and to its cyclic shifts (this results from equating coefficients of $x^k, x^{k+1}, \ldots, x^{n-1}$ must all be zero in $c(x)h(x)$). Thus all the $n-k$ rows are orthogonal to all the codewords and are linearly independent (becuase echelon of $h_k = 1$ in H), and the dimension of $C^\perp$ is also $n-k$. Hence, H is a generator matrix of $C^\perp$. □