Chapter 6

Cyclic Codes

In this chapter we will introduce a special, but still important, class of codes that have a nice mathematical structure. In particular it turns out to be easy to estimate the minimum distance of these codes.

6.1 Introduction to cyclic codes

Definition 6.1.1. *An (n, k) linear code C over $\mathbb{F}_q$ is called* cyclic *if any cyclic shift of a codeword is again a codeword, i.e. if*

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C \Longrightarrow \widehat{c} = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Example 6.1.1. The $(7, 3)$ code over $\mathbb{F}_2$ that consists of the codewords

$$(0, 0, 0, 0, 0, 0, 0), (1, 0, 1, 1, 1, 0, 0), (0, 1, 0, 1, 1, 1, 0), (0, 0, 1, 0, 1, 1, 1),$$
$$(1, 0, 0, 1, 0, 1, 1), (1, 1, 0, 0, 1, 0, 1), (1, 1, 1, 0, 0, 1, 0), (0, 1, 1, 1, 0, 0, 1)$$

can be seen to be a cyclic code.

The properties of cyclic codes are more easily understood if we treat words as polynomials in $\mathbb{F}_q[x]$. This means that if $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ we associate the polynomial $a(x) = a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x]$.

In the following we will not distinguish between codewords and codepolynomials.

The first observation is

Lemma 6.1.1. *If*

$$c(x) = c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \qquad \textit{and} \qquad \widehat{c}(x) = c_{n-2}x^{n-1} + \cdots + c_0x + c_{n-1}$$

then

$$\widehat{c}(x) = xc(x) - c_{n-1}(x^n - 1)$$

The lemma is proved by direct calculation.

Theorem 6.1.1. *Let C be a cyclic (n, k) code over $\mathbb{F}_q$ and let $g(x)$ be the monic polynomial of lowest degree in $C\backslash\{0\}$.*
Then

1. *$g(x)$ divides $c(x)$ for every $c \in C$.*
2. *$g(x)$ divides $x^n - 1$ in $\mathbb{F}_q[x]$.*
3. *$k = n - \deg(g(x))$.*

We first note that $g(x)$ is uniquely determined, since if there were two, their difference (since the code is linear) would have lower degree and would be a codeword.

Proof of the theorem.
It is clear from the definition of $g(x)$ that $k \le n - \deg(g(x))$, since there are only $n - \deg(g(x))$ positions left.

If $g(x)$ has degree s, then $g(x) = g_{s-1}x^{s-1} + \cdots + g_1x + g_0 + x^s$ so from Lemma 6.1.1 we get that $x^j g(x)$ is in C if $j \le n - 1 - s$. Therefore $a(x)g(x)$ where $\deg(a(x)) \le n - 1 - s$ are also codewords of C.

It is also easy to see that $x^j g(x)$ where $j \le n - 1 - s$ are linearly independent codewords of C, so $k \ge n - s$, and we then have $k = n - s$, proving 3.

To prove 1, suppose $c(x) \in C$ then $c(x) = a(x)g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$. Since $\deg(a(x)) \le n - 1 - s$ we have that $a(x)g(x)$ is a codeword and therefore that $r(x) = c(x) - a(x)g(x)$ is also in the code. Since $\deg(r(x)) < \deg(g(x))$ this implies that $r(x) = 0$ and therefore $g(x)$ divides $c(x)$, and 1 is proved.

2 follows directly from the lemma since $g(x)$ divides $c(x)$ and also $\widehat{c}(x)$. □

The polynomial $g(x)$ in the theorem is called the *generator polynomial* for the cyclic code C.

Example 6.1.2. (Example 6.1.1 continued) We see that $g(x) = x^4 + x^3 + x^2 + 1$ and that the codewords all have the form $(a_2x^2 + a_1x + a_0)g(x)$ where $a_i \in \mathbb{F}_2$ and that $x^7 - 1 = (x^4 + x^3 + x^2 + 1)(x^3 + x^2 + 1)$.

So to a cyclic code corresponds a divisor of $x^n - 1$ and a natural question is therefore if there to any divisor of $x^n - 1$ corresponds a cyclic code. We answer that in the affirmative in

Theorem 6.1.2. *Suppose $g(x) \in \mathbb{F}_q[x]$ is monic and divides $x^n - 1$.*
Then $C = \{i(x)g(x) | i(x) \in \mathbb{F}_q[x], \deg(i(x)) < n - \deg(g(x))\}$ is a cyclic code with generator polynomial $g(x)$.

Proof. It is obvious that C is a linear code, and if it is cyclic the generator polynomial is $g(x)$ and hence the dimension is $n - \deg(g(x))$ so we only have to prove that C is cyclic.

To this end let $g(x) = g_{s-1}x^{s-1} + \cdots + g_1x + g_0 + x^s$ and $h(x) = \frac{(x^n-1)}{g(x)} = x^{n-s} + h_{n-s-1}x^{n-s-1} + \cdots + h_1x + h_0$.

Let $c(x) = i(x)g(x)$ where $\deg(i(x)) < n - s$, then

$$\widehat{c}(x) = xc(x) - c_{n-1}(x^n - 1) = xi(x)g(x) - c_{n-1}h(x)g(x) = (xi(x) - c_{n-1}h(x))g(x).$$

Now $c_{n-1} = i_{n-s-1}$ so indeed $(xi(x) - c_{n-1}h(x))$ has deg $< n - s$ and therefore $\widehat{c}(x)$ is also in C. □

The two theorems combined tell us that we can study cyclic codes by studying the divisors of $x^n - 1$. In the case $q = 2$ and n odd we gave a method for finding divisors of $x^n - 1$ in Section 2.3.

Example 6.1.3. Binary cyclic codes of length 21

Using the algorithm of Section 2.3 we have

$$x^{21}-1 = (x-1)(x^6+x^4+x^2+x+1)(x^3+x^2+1)(x^6+x^5+x^4+x^2+1)(x^2+x+1)(x^3+x+1).$$

With $g(x) = (x^6 + x^4 + x^2 + x + 1)(x^3 + x^2 + 1)$ we get a (21, 12) binary code. With $g_1(x) = (x^6 + x^4 + x^2 + x + 1)(x^3 + x + 1)$ we also get a (21, 12) code.

6.2 Generator- and parity check matrices of cyclic codes

Let C be an (n, k) cyclic code over $\mathbb{F}_q$. As proved in Section 6.1 the code C has a generator polynomial $g(x)$ of degree $n - k$, that is $g(x) = x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_1x + g_0$ and we also saw that $x^j g(x)$, $j = 0, 1, \ldots, k - 1$ gave linearly independent codewords. This means that a generatormatrix of C is

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

So G has as its first row the coefficients of $g(x)$ and the remaining $k - 1$ rows are obtained as cyclic shifts.

To get a parity check matrix we observe that $g(x)h(x) = x^n - 1$, since $h(x)$ was defined exactly in this way and, if $c(x) = i(x)g(x)$, we get that $c(x)h(x) = i(x)g(x)h(x) = i(x)(x^n - 1)$ so the polynomial $c(x)h(x)$ does not contain any terms of degrees $k, k + 1, \ldots, n - 1$ and therefore $\sum_{i=0}^{n-1} c_i h_{j-i} = 0$ for $j = k, k+1, \ldots, n-1$, where $h_s = 0$ if $s < 0$.

From this we get that the vectors

$$(h_k, h_{k-1}, \ldots, h_0, 0, \ldots, 0), \ldots, (0, \ldots, h_k, h_{k-1}, \ldots, h_0)$$

give $n - k$ independent parity check equations so a parity check matrix is

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots \\ 0 & h_k & h_{k-1} & \dots \\ 0 & 0 & h_k & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

So H has as its first row the coefficients of $h(x)$ in reverse order and the remaining $n - k - 1$ rows are cyclic shifts of the first row. Therefore we have

Theorem 6.2.1. *If C is an (n, k) cyclic code with generator polynomial $g(x)$, then the dual code $C^{\perp}$ is also cyclic and has generator polynomial $g^{\perp}(x) = h_0 x^k + \cdots + h_{k-1}x + h_k = x^k h(x^{-1})$ where $h(x) = \frac{x^n-1}{g(x)}$*

Example 6.2.1. For the code considered in Example 6.1.1 we get

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

and

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

6.3 A theorem on the minimum distance of cyclic codes

In this section we prove a lower bound on the minimum distance of a cyclic code (the so-called BCH-bound).

Theorem 6.3.1. *Let $g(x)$ be the generator polynomial of a cyclic (n, k) code C over $\mathbb{F}_q$ and suppose that $g(x)$ has among its zeroes $\beta^a, \beta^{a+1}, \dots, \beta^{a+d-2}$ where $\beta \in \mathbb{F}_q^m$ has order n.*

Then $d_{min}(C) \geq d$.

Proof.

$$H = \begin{pmatrix} 1 & \beta^a & \beta^{2a} & \dots & \beta^{a(n-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \beta^{a+d-2} & \beta^{2(a+d-2)} & \dots & \beta^{(n-1)(a+d-2)} \end{pmatrix}$$