CYCLIC CODES

Example of a Simple Cyclic Code Consider the binary code

\[ C = \{000, 110, 011, 101\}. \]

One easily checks that this is a linear code since the sum of any two codewords in \( C \) is again a codeword in \( C \). Let us denote a codeword in \( C \) by \( c = (c_1, c_2, c_3) \) where \( c_i \) is either 0 or 1 for \( i = 1, 2, 3 \).

The key property that makes this a cyclic code is that for any codeword \( c = (c_1, c_2, c_3) \in C \) we have \( (c_3, c_1, c_2) \) is again a codeword in \( C \).

Definition (Cyclic Code) A binary code is cyclic if it is a linear \([n, k]\) code and if for every codeword \((c_1, c_2, \ldots, c_n) \in C\) we also have that \((c_n, c_1, \ldots, c_{n-1})\) is again a codeword in \( C \).

Remark: The shift \((c_1, c_2, \ldots, c_n) \rightarrow (c_n, c_1, \ldots, c_{n-1})\) is called a right cyclic shift.

Question: Is \(\{000, 100, 010, 001\}\) a cyclic code?

Answer: The answer is NO because this code is not linear.

REALIZING CYCLIC CODES WITH POLYNOMIALS OVER \( \mathbb{F}_2 \)

In the following we let \( \mathbb{F}_2[x] \) denote the set of all polynomials

\[ a_0 + a_1 x + \cdots + a_m x^m \]

with \( a_i \in \mathbb{F}_2 \) for \( i = 0, 1, \ldots, m \). We note that these polynomials form an additive group.

Definition (Code Polynomial associated to a Cyclic Codeword) Let \( a = (a_0, a_1, \ldots, a_{n-1}) \) be a codeword in a cyclic \([n, k]\) code \( C \). We define the polynomial associated to \( a \in C \) to be

\[ a(x) := a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_2[x]. \]

Notice that

\[ x \cdot a(x) = a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} + a_{n-1} x^n. \]

This is almost a right cyclic shift of the polynomial which would have the representation

\[ a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1}. \]

But notice the following identity!

\[ x \cdot a(x) \equiv a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} \pmod{(x^n - 1)}. \]  \hfill (1)

Furthermore, it immediately follows that we also have:

\[ x^2 \cdot a(x) \equiv a_{n-2} + a_{n-1} x + a_0 x^2 + a_1 x^3 + \cdots + a_{n-3} x^{n-1} \pmod{(x^n - 1)} \]

\[ x^3 \cdot a(x) \equiv a_{n-3} + a_{n-2} x + a_{n-1} x^2 + a_0 x^3 + \cdots + a_{n-4} x^{n-1} \pmod{(x^n - 1)} \]

\[ \vdots \]

\[ x^\ell \cdot a(x) \equiv a_{n-\ell} + a_{n-\ell+1} x + a_{n-\ell+2} x^2 + \cdots + a_0 x^\ell + \cdots + a_{n-\ell-1} x^{n-1} \pmod{(x^n - 1)}. \]

Remark: The numbering \( a = (a_0, a_1, \ldots, a_{n-1}) \) starting with \( a_0 \) instead of \( a_1 \) is used because it simplifies the statement of the modular relation (1).
CONSTRUCTING CYCLIC CODES WITH POLYNOMIALS OVER $\mathbb{F}_2$

**Claim:** Fix an integer $n > 1$. Let $g(x) \in \mathbb{F}_2[x]$ divide the polynomial $x^n - 1$. Assume the degree of $g(x)$ is $n - k$ for some $0 \leq k \leq n$. Consider the set of polynomials

$$\mathcal{P}_g := \{g(x) \cdot \alpha(x) \mod (x^n - 1) \mid \alpha(x) \in \mathbb{F}_2[x] \text{ with } \deg(\alpha(x)) \leq k\}.$$ 

Every polynomial $f(x) \in \mathcal{P}_g$ can be written in the form

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$ 

Then the set of all distinct $\{a_0, a_1, \ldots, a_{n-1}\}$ coming from $f(x) \in \mathcal{P}_g$ form a cyclic $[n, k]$ code.

**Remark:** The polynomial $g$ is called a generator polynomial for the cyclic $[n, k]$ code described in the above theorem.

**Example (1):** Let $n = 3$. Then $g(x) := x - 1$ divides $x^3 - 1$. Note that since we are over $\mathbb{F}_2$ we see that $g(x)$ is also equal to $1 + x$. We now list all possible

$$g(x) \cdot \alpha(x) \mod (x^3 - 1)$$

with $\deg(\alpha(x)) \leq 1$. The only possible $\alpha(x)$ are $0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2$. Furthermore

$$x^3 \equiv 1 \mod (x^3 - 1).$$

It follows that for this example

$$(1 + x) \cdot 0 \equiv 0 \mod (x^3 - 1) \rightarrow 000,$n

$$(1 + x) \cdot 1 \equiv 1 + x \mod (x^3 - 1) \rightarrow 110,$n

$$(1 + x) \cdot x \equiv x + x^2 \mod (x^3 - 1) \rightarrow 011,$n

$$(1 + x) \cdot (1 + x) \equiv 1 + x^2 \mod (x^3 - 1) \rightarrow 101,$n

$$(1 + x) \cdot x^2 \equiv 1 + x^2 \mod (x^3 - 1) \rightarrow 101,$n

$$(1 + x) \cdot (1 + x^2) \equiv x + x^2 \mod (x^3 - 1) \rightarrow 011,$n

$$(1 + x) \cdot (x + x^2) \equiv 1 + x \mod (x^3 - 1) \rightarrow 110,$n

$$(1 + x) \cdot (1 + x + x^2) \equiv 0 \mod (x^3 - 1) \rightarrow 000,$n

In the above we have taken a polynomial such as $x + x^2$ and rewritten it as the codeword $\rightarrow 011$.

We see that we get the codewords $\{000, 101, 110, 011\}$ which is a cyclic code. So the above **Claim** holds for this example.

**Remark:** Note that in the above calculation we obtained each codeword in $\{000, 101, 110, 011\}$ exactly twice. This suggests that it is enough to consider polynomials $\alpha(x) \in \mathbb{F}_2[x]$ with $\deg(\alpha(x)) < k$.

**Explanation of why each code word is repeated twice:**

We have $(1 + x) \cdot (1 + x + x^2) = x^3 - 1$. Hence $(1 + x) \cdot x^2 \equiv (1 + x)^2 \equiv 1 + x^2 \mod (x^3 - 1)$. This means that $(1 + x) \cdot x^2$ is in the list of the first four code polynomials. It follows that $(1 + x) \cdot (1 + x^2)$ and $(1 + x) \cdot (x + x^2)$ and $(1 + x) \cdot (1 + x + x^2) \equiv 0$ must also be in the list of the first four code polynomials.
Example (2): Let’s take \( n = 3 \) and \( g(x) := 1 + x + x^2 \) which also divides \( 1 + x^3 \) since \( 1 + x^3 = (1 + x) \cdot (1 + x + x^2) \). Note that we defined \( k \) so that \( \deg(g(x)) = n - k \). It follows that since \( g(x) \) has degree 2 that \( k = 1 \). In this case there are only four possible polynomials \( \alpha(x) \) of degree \( \leq k = 1 \). These are \( \{0, 1, x, 1 + x\} \). It follows that
\[
\begin{align*}
(1 + x + x^2) \cdot 0 & \equiv 0 \pmod{x^3 - 1} \quad \rightarrow 000, \\
(1 + x + x^2) \cdot 1 & \equiv 1 + x + x^2 \pmod{x^3 - 1} \quad \rightarrow 111, \\
(1 + x + x^2) \cdot x & \equiv 1 + x + x^2 \pmod{x^3 - 1} \quad \rightarrow 111, \\
(1 + x + x^2) \cdot (1 + x) & \equiv 0 \pmod{x^3 - 1} \quad \rightarrow 000,
\end{align*}
\]
We see that the code generated is the \([3,1]\) repetition code which is just \( \{000,111\} \). The codewords are repeated exactly twice.

We will now prove the following theorem.

Theorem (1): Fix an integer \( n > 1 \). Let \( g(x) \in \mathbb{F}_2[x] \) divide the polynomial \( x^n - 1 \). Assume the degree of \( g(x) \) is \( n - k \) for some \( 0 \leq k \leq n \). Consider the set of polynomials
\[
\mathcal{P}_g := \left\{ g(x) \cdot \alpha(x) \pmod{x^n - 1} \mid \alpha(x) \in \mathbb{F}_2[x] \text{ with } \deg(\alpha(x)) < k \right\}.
\]
Every code polynomial \( f(x) \in \mathcal{P}_g \) can be written in the form
\[
f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.
\]
Then the set of all \( \{a_0, a_1, \ldots, a_{n-1}\} \) coming from \( f(x) \in \mathcal{P}_g \) form a cyclic \([n,k]\) code.

Remark Note that the difference between Theorem (1) and the CLAIM on the previous page is that we only need polynomials \( \alpha(x) \) with \( \deg(\alpha(x)) < k \). In the CLAIM we had \( \deg(\alpha(x)) \leq k \).

Proof of Theorem (1): Let \( C \) denote the code generated in the above theorem. First of all every codeword in \( C \) is associated to a code polynomial of the form \( g(x) \cdot \alpha(x) \) where \( \alpha(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} \in \mathbb{F}_2[x] \) is a polynomial of degree \( < k \). It follows that the sum of any two codewords is again a codeword since the sum of any two polynomials of degree \( < k \) must again be a polynomial of degree \( < k \).

It remains to prove that the code \( C \) is cyclic. Let \( f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{P}_g \). Then we may write
\[
x \cdot f(x) = a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n
= a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}(x^n + 1)
= h(x) + a_{n-1}(x^n + 1).
\]
Since both \( x \cdot f(x) \) and \( x^n + 1 \) are divisible by \( g(x) \) it follows that \( h(x) \) must also be divisible by \( g(x) \). Hence \( h(x) \) (which represents the cyclic right shift of \( f(x) \)) must also be a code polynomial in \( \mathcal{P}_g \), and the code generated by \( g(x) \) is a cyclic code. \( \square \)
We shall next prove that every cyclic code can be constructed (as in Theorem (1)) from a generating polynomial \( g(x) \) which divides \( x^n - 1 \).

**Theorem (2):** Let \( C \) be a cyclic code. Then there exists a uniquely determined code polynomial \( g(x) \) of minimal degree in \( C \) which has the following properties.

(i) \( g(x) \) is unique.

(ii) \( g(x) \) divides \( x^n - 1 \).

(iii) The code \( C \) can be constructed using \( g(x) \) as in Theorem (1).

The polynomial \( g(x) \) is called the generator polynomial for the code \( C \).

**Proof of Theorem (2):**

(i) Assume there are two distinct code polynomials \( g_1(x), g_2(x) \) of minimal degree in \( C \). Then \( g_1(x) - g_2(x) \) will have a smaller degree than \( g_1(x) \) or \( g_2(x) \). This is a contradiction so the polynomial \( g(x) \) of minimal degree must be unique.

(ii) Next, assume \( g(x) \) does not divide \( x^n - 1 \). Then

\[
x^n - 1 = g(x)\beta(x) + r(x), \quad (\beta(x), r(x) \in F_2[x]),
\]

where \( r(x) \) is the remainder polynomial which must have degree smaller than \( g(x) \). This implies \( r(x) \) is also a code polynomial of smaller degree than \( g(x) \) which is a contradiction.

(iii) Once we have found \( g(x) \) it follows from (i), (ii), that we may construct the code \( C \) as in Theorem (1). \( \square \)

**HOW TO FIND ALL \([7,k]\) CYCLIC CODES**

We first factor \( x^7 - 1 = (x - 1) \cdot (x^3 + x + 1) \cdot (x^2 + x^2 + 1) \). Since we are only considering binary codes (where +1 is the same as -1), we can rewrite the factorization as \( 1 + x^7 = (1 + x) \cdot (1 + x + x^3) \cdot (1 + x^2 + x^3) \). As there are 3 irreducible factors there are 8 cyclic codes (including 0 and \( F_7^2 \)) with the following generator polynomials:

1. \( g(x) = 1, \quad C = F_2^7 = [7, 7] \) code
2. \( g(x) = 1 + x, \quad C = [7, 6] \) code
3. \( g(x) = 1 + x + x^3, \quad C = [7, 4] \) code
4. \( g(x) = 1 + x^2 + x^3, \quad C = [7, 4] \) code
5. \( g(x) = (1 + x)(1 + x + x^3) = 1 + x^2 + x^3 + x^4, \quad C = [7, 3] \) code
6. \( g(x) = (1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4, \quad C = [7, 3] \) code
7. \( g(x) = (1 + x + x^3)(1 + x^2 + x^3) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6, \quad C = [7, 1] \) code
8. \( g(x) = x^7 + 1, \quad C = \{0000000\} = [7, 0] \) code.