Coding Theory: Cyclic Codes

Cyclic Codes

A linear code $\mathcal{C}$ of length n such that for each vector $\mathbf{c} = (c_0, \ldots, c_{n-1})$ in $\mathcal{C}$, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ in $\mathcal{C}$.

- Note that indices are from 0 to $n-1$, this is because it is convenient to think of positions in terms of integers modulo n: shift means $i \mapsto i+1 \pmod{n}$.
- In words, a cyclic code of length n contains all n cyclic shifts of any codeword.

Exercise. (1) Give one example of a cyclic code. (2) Is the $(n, n-1)$ single-parity check code cyclic?

Exercise. (1) Give one example of a cyclic code. (2) Is the $(n, n-1)$ single-parity check code cyclic?

(1) We could take the repetition code. Indeed, all shifts of the zero vector $(0, 0, \ldots, 0)$ are in the code (it is the same vector), the same holds for the whole 1 vector $(1, 1, \ldots, 1)$.

Exercise. (1) Give one example of a cyclic code. (2) Is the $(n, n-1)$ single-parity check code cyclic?

(1) We could take the repetition code. Indeed, all shifts of the zero vector $(0, 0, \ldots, 0)$ are in the code (it is the same vector), the same holds for the whole 1 vector $(1, 1, \ldots, 1)$.

(2) Take a generic codeword $(c_0, \ldots, c_{n-3}, c_{n-2}, \sum_{i=0}^{n-1} c_i)$. A shift gives the codeword $(\sum_{i=0}^{n-1} c_i, c_0, \ldots, c_{n-3}, c_{n-2})$. To know whether the shifted codeword belongs to the code, we recall that it must satisfy that the last coefficient is the sum of the previous ones, which is true.

We often represent the codewords in polynomial form:

$$\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n \iff c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \in \mathbb{F}_q[X]$$

We often represent the codewords in polynomial form:

$$\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n \Longleftrightarrow c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \in \mathbb{F}_q[X]$$

If $c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$, then
$X c(X) = c_0 X + c_1 X^2 + \ldots + c_{n-1} X^n \equiv$
$c_{n-1} + c_0 X + c_1 X^2 + \ldots + c_{n-2} X^{n-1} \pmod{X^n - 1}$.

We often represent the codewords in polynomial form:

$$\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n \Longleftrightarrow c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \in \mathbb{F}_q[X]$$

If $c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$, then
$Xc(X) = c_0 X + c_1 X^2 + \ldots + c_{n-1} X^n \equiv$
$c_{n-1} + c_0 X + c_1 X^2 + \ldots + c_{n-2} X^{n-1} \pmod{X^n - 1}$.

In a cyclic code $\mathcal{C}$, if $c(X) \in \mathcal{C}$, so is $Xc(X) \pmod{X^n - 1}$.

In a cyclic code $\mathcal{C}$, if $c(X) \in \mathcal{C}$, so is $Xc(X) \pmod{X^n - 1}$.

In a cyclic code $\mathcal{C}$, if $c(X) \in \mathcal{C}$, so is $Xc(X) \pmod{X^n - 1}$.

But then, if $Xc(X) \pmod{X^n - 1}$ is a codeword, so must be $X^2c(X) \pmod{X^n - 1}$.

In a cyclic code $\mathcal{C}$, if $c(X) \in \mathcal{C}$, so is $Xc(X) \pmod{X^n - 1}$.

But then, if $Xc(X) \pmod{X^n - 1}$ is a codeword, so must be $X^2c(X) \pmod{X^n - 1}$.

Since the code is linear, whenever a codeword is in $\mathcal{C}$, so are its multiples.

Let $\mathcal{C}$ be an (n,k) cyclic code. If $c(X) \in \mathcal{C}$, then for any polynomial $p(X) \in \mathbb{F}_q[X]$, $p(X)c(X) \pmod{X^n - 1}$ is also a codeword in $\mathcal{C}$.

Suppose $p(X) = \sum_{i=0}^{k} p_i X^i$.

$p(X)c(X) = (\sum_{i=0}^{k} p_i X^i)c(X) = \sum_{i=0}^{k} p_i(X^i c(X))$. Modulo $\pmod{X^n - 1}$, $X^i c(X)$ is a codeword, and since the code is linear, a linear combination of codewords is a codeword.

Exercise. Consider the binary code generated by

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

(1) Show that this code is cyclic. (2) Illustrate the claim of the previous slide on this example (choose any codeword and polynomial you like).

Exercise. Consider the binary code generated by

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

(1) To show that the code is cyclic, we need to show that for every codeword, all its shifts are in the code. Since the code is binary of dimension $k = 3$, it contains 8 codewords:

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

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

For every codeword, we need to see that all shifts are here:

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

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

$$(1,0,1,1,1,0,0) \xrightarrow{shift} (0,1,0,1,1,1,0) \xrightarrow{shift}$$
$$(0,0,1,0,1,1,1) \xrightarrow{shift} (1,0,0,1,0,1,1) \xrightarrow{shift}$$
$$(1,1,0,0,1,0,1) \xrightarrow{shift} (1,1,1,0,0,1,0) \xrightarrow{shift} (0,1,1,1,0,0,1)$$

Exercise. Consider the binary code generated by

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

(2) Illustrate the claim of the previous slide on this example.

---

(2) Take for example $(1, 0, 0, 1, 0, 1, 1)$, as a polynomial it is $1 + X^3 + X^5 + X^6$. Take some polynomial say $X + 1$. Then

$$(1+X)(1+X^3+X^5+X^6) = 1+X^3+X^5+X^6+X+X^4+X^6+X^7.$$

The code has length $n = 7$, so modulo $X^7 - 1$, we get

$$1 + X + X^3 + X^4 + X^5 + X^6 + X^6 + 1 \equiv X + X^3 + X^4 + X^5.$$

As a codeword, this is $(0, 1, 0, 1, 1, 1, 0)$, indeed in the code.

The right framework for linear cyclic codes of length n is to consider

$$\mathbb{F}_q[X]/(X^n - 1).$$

In this set, we have polynomials modulo $X^n - 1$, with a multiplication modulo $X^n - 1$.

Generator polynomial of a cyclic code.

For $\mathcal{C}$ a cyclic code, a nonzero polynomial $g(X)$ of lowest degree in $\mathcal{C}$.

Let us continue our previous example with 8 codewords: $(0,0,0,0,0,0,0)$, $(1,0,1,1,1,0,0)$, $(0,1,0,1,1,1,0)$, $(0,0,1,0,1,1,1)$, $(1,1,1,0,0,1,0)$, $(1,0,0,1,0,1,1)$, $(0,1,1,1,0,0,1)$, $(1,1,0,0,1,0,1)$.

Generator polynomial of a cyclic code.

For $\mathcal{C}$ a cyclic code, a nonzero polynomial $g(X)$ of lowest degree in $\mathcal{C}$.

Let us continue our previous example with 8 codewords: $(0,0,0,0,0,0,0), (1,0,1,1,1,0,0), (0,1,0,1,1,1,0), (0,0,1,0,1,1,1), (1,1,1,0,0,1,0), (1,0,0,1,0,1,1), (0,1,1,1,0,0,1), (1,1,0,0,1,0,1)$.

- $(1,0,1,1,1,0,0)$ has lowest degree.

Generator polynomial of a cyclic code.

For $\mathcal{C}$ a cyclic code, a nonzero polynomial $g(X)$ of lowest degree in $\mathcal{C}$.

Let us continue our previous example with 8 codewords: $(0,0,0,0,0,0,0),(1,0,1,1,1,0,0),(0,1,0,1,1,1,0),(0,0,1,0,1,1,1),(1,1,1,0,0,1,0),(1,0,0,1,0,1,1),(0,1,1,1,0,0,1),(1,1,0,0,1,0,1)$.

- $(1,0,1,1,1,0,0)$ has lowest degree.

We saw all the shifts of $(1,0,1,1,1,0,0)$ generate all non-zero codewords of the code.

Generator polynomial of a cyclic code.

For $\mathcal{C}$ a linear cyclic code, a nonzero polynomial $g(X)$ of lowest degree r in $\mathcal{C}$. Taking $g(X)$ monic, we refer to the generator polynomial.
Then
$\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X], \deg(q(X)) < n - r\}$.

The set
$\mathcal{C}_0 = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X],\ \deg(q(X)) < n - r\}$ is contained in $\mathcal{C}$ (we know codewords multiplied by polynomials are in $\mathcal{C}$).
Left to prove: $\mathcal{C}$ is contained in $\mathcal{C}_0$.

Generator polynomial of a cyclic code.

For $\mathcal{C}$ a linear cyclic code, the nonzero monic polynomial $g(X)$ of lowest degree r in $\mathcal{C}$.
To prove: $\mathcal{C} \subset \mathcal{C}_0 = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X],\ \deg(q(X)) < n-r\}$.

Take $c(X)$ any polynomial in $\mathcal{C}$ and do a Euclidean division:
$\underbrace{c(X)}_{\in\mathcal{C}} = \underbrace{g(X)q(X)}_{\in\mathcal{C}_0} + r(X)$, with
$\deg r(X) < \deg g(X)$ or $r(X) = 0$.
Since $g(X)$ has the lowest degree, $r(X) = 0$ and $c(X) = g(X)q(X)$.

Exercise. Consider the binary code $\mathcal{C}$ generated by

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

Find its generator polynomial and check that indeed $\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X],\ \deg(q(X)) < n - r\}$ where r is the degree of the polynomial.

Exercise. Consider the binary code $\mathcal{C}$ generated by

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

Find its generator polynomial and check that indeed $\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X],\ \deg(q(X)) < n - r\}$ where r is the degree of the polynomial.

To find the generator polynomial, we need the codeword whose polynomial is of lowest degree (it will be monic since it is a binary code). We already computed it, it is $g(X) = 1 + X^2 + X^3 + X^4$.

Exercise. Check that indeed
$\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X],\ \deg(q(X)) < n - r\}$ where r is the degree of the polynomial.

Exercise. Check that indeed
$\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X],\ \deg(q(X)) < n - r\}$ where r is the degree of the polynomial.

Since the generator polynomial is $g(X) = 1 + X^2 + X^3 + X^4$, $r = 4$ and $n = 7$ so $n - r = 7 - 4 = 3$. So $q(X) = q_0 + q_1 X + q_2 X^2$ so we have 8 such polynomials (which is good, we have 8 codewords).
We have $q(X)g(X) = (q_0 + q_1 X + q_2 X^2)(1 + X^2 + X^3 + X^4) = q_0 + q_0 X^2 + q_0 X^3 + q_0 X^4 + q_1 X + q_1 X^3 + q_1 X^4 + q_1 X^5 + q_2 X^2 + q_2 X^4 + q_2 X^5 + q_2 X^6$.

We have
$q(X)g(X) = (q_0 + q_1 X + q_2 X^2)(1 + X^2 + X^3 + X^4) = q_0 + q_1 X + X^2(q_0 + q_2) + X^3(q_0 + q_1) + X^4(q_0 + q_1 + q_2) + X^5(q_1 + q_2) + q_2 X^6.$

q_0	q_1	q_2	$q(X)g(X)$	codeword
0	0	0	0	$(0,0,0,0,0,0,0)$
1	0	0	$1 + X^2 + X^3 + X^4$	$(1,0,1,1,1,0,0)$
0	1	0	$X + X^3 + X^4 + X^5$	$(0,1,0,1,1,1,0)$
1	1	0	$1 + X + X^2 + X^5$	$(1,1,1,0,0,1,0)$
0	0	1	$X^2 + X^4 + X^5 + X^6$	$(0,0,1,0,1,1,1)$
1	0	1	$1 + X^3 + X^5 + X^6$	$(1,0,0,1,0,1,1)$
0	1	1	$X + X^2 + X^3 + X^6$	$(0,1,1,1,0,0,1)$
1	1	1	$1 + X + X^4 + X^6$	$(1,1,0,0,1,0,1)$

Definition of cyclic code

Correspondance between codeword and polynomial

Generator polynomial