Coding Theory: Cyclic Codes (II)

- A linear cyclic code $\mathcal{C}$ of length n contains all n cyclic shifts of any codeword.
- $\mathbf{c} = (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n \Longleftrightarrow c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \in \mathbb{F}_q[X]$
- $\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X], \deg(q(X)) < n - r\}$, where $g(X)$ is the monic polynomial of lowest degree r in $\mathcal{C}$ called the generator polynomial.

Dimension of a linear (n, k) cyclic code

If $\deg g(X) = r$,
$k = n - r$.

- $\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X], \deg(q(X)) < n - r\}$
It is a vector space of dimension $n - r$ over $\mathbb{F}_q$.

Consider the $(7,3)$ linear binary code $\mathcal{C}$ generated by

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

$\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X],\ \deg(q(X)) < n - r\}$ where $q(X)g(X) = (q_0 + q_1X + q_2X^2)(1 + X^2 + X^3 + X^4) = q_0 + q_1X + X^2(q_0 + q_2) + X^3(q_0 + q_1) + X^4(q_0 + q_1 + q_2) + X^5(q_1 + q_2) + q_2X^6$.

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	$1+X+X^4+X^6$	$(1,1,0,0,1,0,1)$

The generator polynomial $g(X)$ divides $X^n - 1$ in $\mathbb{F}_q[X]$.

Divide $X^n - 1$ by $g(X)$:

$$X^n - 1 = g(X)h(X) + s(X)$$

with
$\deg s(X) < \deg g(X)$.

Then $\pmod{X^n - 1}$

$$s(X) = \underbrace{(-h(X))g(X)}_{\in \mathcal{C}}$$

so $s(X)$ must be zero and

$$g(X)h(X) = X^n - 1.$$

We call $h(X)$ the check polynomial.

Exercise. We continue with the $(7, 3)$ cyclic code, with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$. Find its check polynomial $h(X)$.

Exercise. We continue with the $(7,3)$ cyclic code, with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$. Find its check polynomial $h(X)$.

We need a polynomial $h(X)$ such that $h(X)g(X) = X^7 - 1 \in \mathbb{F}_2[X]$. Then

$$(\underbrace{h_0}_{1} + h_1 X + h_2 X^2 + \underbrace{h_3}_{1} X^3)(1 + X^2 + X^3 + X^4) = X^7 - 1.$$

Exercise. We continue with the $(7,3)$ cyclic code, with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$. Find its check polynomial $h(X)$.

We need a polynomial $h(X)$ such that $h(X)g(X) = X^7 - 1 \in \mathbb{F}_2[X]$. Then

$$(\underbrace{h_0}_{1} + h_1 X + h_2 X^2 + \underbrace{h_3}_{1} X^3)(1 + X^2 + X^3 + X^4) = X^7 - 1.$$

$1 + h_1 X + X^2(1 + h_2) + h_1 X^3 + X^4(1 + h_1 + h_2) + X^5(h_1 + h_2 + 1) + X^6(h_2 + 1) + X^7 = X^7 - 1.$
Then $(1 + X^2 + X^3)(1 + X^2 + X^3 + X^4) = X^7 - 1.$

Let $\mathcal{C}$ be a cyclic code of length n and generator polynomial $g(X) = \sum_{i=0}^{r} g_i X^i$ of degree r:

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_{r-1} & g_r & 0 & \dots & 0 & \\ 0 & g_0 & g_1 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & & & & & \\ 0 & & 0 & g_0 & g_1 & & g_{r-1} & g_r & \end{bmatrix}$$

The matrix G has n columns and $k = n - r$ rows. Each row is the cyclic shift of the previous row.
Since $g_0 \neq 0$ since $g(X)h(X) = X^n - 1$, G is in echelon form, its rows are linearly independent thus $k = n - r$ is the dimension of the code generated by G.
The rows of G belong to $\mathcal{C}$ so G is a generator matrix for $\mathcal{C}$.

Exercise. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$. Construct its generator matrix.

Exercise. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$. Construct its generator matrix.

We know that G is obtained by putting on its first row $g_0, g_1, g_2, g_3, g_4, 0, 0$ and then by creating cyclic shifts of this row:

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

For a linear (n, k) cyclic code with generator polynomial $g(X)$ of degree r:

- ✓ Length is n.
- ✓ Dimension is $k = n - r$.
- ✓ Generator matrix is obtained by shifts of the coefficients of $g(X)$.

We notice the critical role of $g(X)$, so we prove one more result about $g(X)$.

If $g(X)$ is a divisor of $X^n - 1$, then $g(X)$ is the generator polynomial of an (n, k) cyclic code.

Suppose $g(X)|X^n - 1$. We consider the set $q(X)g(X)$ of multiples of $g(X)$. This forms an (n, k) linear code, where $k = n - \deg g(X)$. We need to show it is cyclic.

Let $q(X)g(X)$ be a codeword. A shift is of the form $Xq(X)g(X) \pmod{X^n - 1}$. Since $g(X)|X^n - 1$, $X^n - 1 = g(X)s(X)$, thus $(Xq(X)g(X) \pmod{X^n - 1}) \pmod{g(X)} \equiv Xq(X)g(X) \pmod{g(X)} \equiv 0$ so $Xq(X)g(X) \pmod{X^n - 1}$ is a multiple of $g(X)$ and the code is indeed cyclic.

For a linear (n, k) cyclic code with generator polynomial $g(X)$ of degree r:

- ✓ Length is n.
- ✓ Dimension is $k = n - r$.
- ✓ Generator matrix is obtained by shifts of the coefficients of $g(X)$.

There is a correspondance between divisors $g(X)$ of $X^n - 1$ and cyclic codes of length n.

Systematic form

We want to send a message $m(X) = (m_0, \ldots, m_{k-1})$, and encode it into $c(X) = (m_0, \ldots, m_{k-1}, ?, \ldots, ?)$.

Compute $X^r m(X)$ and

$$X^r m(X) = q(X)g(X) + s(X),$$

$\deg(s(X)) < r$. Then

$$X^r m(X) - s(X) = \underbrace{q(X)g(X)}_{\in \mathcal{C}}$$

so $X^r m(X) - s(X)$ is a codeword written

$$(-s_0, \ldots, -s_{r-1}, m_0, \ldots, m_{k-1}).$$

For a linear (n, k) cyclic code with generator polynomial $g(X)$ of degree r:

- $(-s_0, \dots, -s_{r-1}, m_0, \dots, m_{k-1})$ is a codeword, and since every cyclic shift is also a codeword, this codeword can be shifted of k right shift to obtain codeword $(m_0, \dots, m_{k-1}, -s_0, \dots, -s_{r-1})$.
- To construct a generator matrix in systematic form, encode the message polynomials $m(X) = X^i$ for $i = 0, \dots, k-1$.

Example. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$.

Example. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$.

We encode the message polynomials $m(X) = X^i$ for $i = 0, \ldots, k-1$, $k = n - r = 7 - 4 = 3$.

$$\begin{aligned}
X^4X^0 &= X^4 = g(X) + 1 + X^2 + X^3 \\
X^4X^1 &= X^5 = Xg(X) + X + X^3 + X^4 \\
&= Xg(X) + X + X^3 + (g(X) + 1 + X^2 + X^3) \\
&= g(X)(X+1) + 1 + X + X^2 \\
X^4X^2 &= X^6 = g(X)(X^2 + X) + X + X^2 + X^3
\end{aligned}$$

We have written $X^rX^i = q(X)g(X) + s(X)$ for $i = 0, 1, 2$.

Example. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$.

We encode the message polynomials $m(X) = X^i$ for $i = 0, 1, 2$, to get $X^r X^i - s(X)$:

$$X^4 + (1 + X^2 + X^3),\ X^5 + (1 + X + X^2),\ X^6 + (X + X^2 + X^3).$$

Example. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$.

We encode the message polynomials $m(X) = X^i$ for $i = 0, 1, 2$, to get $X^r X^i - s(X)$:

$$X^4 + (1 + X^2 + X^3),\ X^5 + (1 + X + X^2),\ X^6 + (X + X^2 + X^3).$$

Thus we get:

$$\begin{array}{ccc} (1,0,1,1|1,0,0) & \to & (1,0,0|1,0,1,1) \\ (1,1,1,0|0,1,0) & \to & (0,1,0|1,1,1,0) \\ (0,1,1,1|0,0,1) & \to & (0,0,1|0,1,1,1) \end{array}$$

with $k = 3$ right shifts.

Example. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$.

From

$$\begin{array}{rcl} (1,0,1,1|1,0,0) & \to & (1,0,0|1,0,1,1) \\ (1,1,1,0|0,1,0) & \to & (0,1,0|1,1,1,0) \\ (0,1,1,1|0,0,1) & \to & (0,0,1|0,1,1,1) \end{array}$$

we get the generator matrix

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

Example. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$.

We already know that G is obtained by putting on its first row $g_0, g_1, g_2, g_3, g_4, 0, 0$ and then by creating cyclic shifts of this row:

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

for its systematic form, and of course both methods give the same results.

Dimension of cyclic codes

Generator matrix

Correspondance between divisors and cyclic codes