Cyclic Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

August 26, 2014

Cyclic Codes

Definition

A cyclic shift of a vector $\begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \end{bmatrix}$ is the vector $\begin{bmatrix} v_{n-1} & v_0 & v_1 & \cdots & v_{n-3} & v_{n-2} \end{bmatrix}$.

Definition

An (n, k) linear block code C is a cyclic code if every cyclic shift of a codeword in C is also a codeword.

Example

Consider the $(7, 4)$ code C with generator matrix

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

Polynomial Representation of Vectors

For every vector $\mathbf{v} = \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \end{bmatrix}$ there is a polynomial

$$\mathbf{v}(X) = v_0 + v_1 X + v_2 X^2 + \cdots + v_{n-1} X^{n-1}$$

Let $\mathbf{v}^{(i)}$ be the vector resulting from i cyclic shifts on $\mathbf{v}$

$$\mathbf{v}^{(i)}(X) = v_{n-i} + v_{n-i+1} X + \cdots + v_{n-1} X^{i-1} + v_0 X^i + \cdots + v_{n-i-1} X^{n-1}$$

Example

$\mathbf{v} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$, $\mathbf{v}(X) = 1 + X^3 + X^4 + X^6$
$\mathbf{v}^{(1)} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$, $\mathbf{v}^{(1)}(X) = 1 + X + X^4 + X^5$
$\mathbf{v}^{(2)} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$, $\mathbf{v}^{(2)}(X) = X + X^2 + X^5 + X^6$

Polynomial Representation of Vectors

- Consider $\mathbf{v}(X)$ and $\mathbf{v}^{(1)}(X)$

$$
\begin{aligned}
\mathbf{v}(X) &= v_0 + v_1 X + v_2 X^2 + \cdots + v_{n-1} X^{n-1} \\
\mathbf{v}^{(1)}(X) &= v_{n-1} + v_0 X + v_1 X^2 + v_2 X^3 + \cdots + v_{n-2} X^{n-2} \\
&= v_{n-1} + X \left[v_0 + v_1 X + v_2 X^2 + \cdots + v_{n-2} X^{n-2} \right] \\
&= v_{n-1}(1 + X^n) + X \left[v_0 + \cdots + v_{n-2} X^{n-2} + v_{n-1} X^{n-1} \right] \\
&= v_{n-1}(1 + X^n) + X\mathbf{v}(X)
\end{aligned}
$$

- In general, $\mathbf{v}(X)$ and $\mathbf{v}^{(i)}(X)$ are related by

$$
X^i \mathbf{v}(X) = \mathbf{v}^{(i)}(X) + \mathbf{q}(X)\left(X^n + 1\right)
$$

  where $\mathbf{q}(X) = v_{n-i} + v_{n-i+1} X + \cdots + v_{n-1} X^{i-1}$
- $\mathbf{v}^{(i)}(X)$ is the remainder when $X^i \mathbf{v}(X)$ is divided by $X^n + 1$

Hamming Code of Length 7

Codeword	Code Polynomial
0000000	0
1000110	$1 + X^4 + X^5$
0100011	$X + X^5 + X^6$
1100101	$1 + X + X^4 + X^6$
0010111	$X^2 + X^4 + X^5 + X^6$
1010001	$1 + X^2 + X^6$
0110100	$X + X^2 + X^4$
1110010	$1 + X + X^2 + X^5$
0001101	$X^3 + X^4 + X^6$
1001011	$1 + X^3 + X^5 + X^6$
0101110	$X + X^3 + X^4 + X^5$
1101000	$1 + X + X^3$
0011010	$X^2 + X^3 + X^5$
1011100	$1 + X^2 + X^3 + X^4$
0111001	$X + X^2 + X^3 + X^6$
1111111	$1 + X + X^2 + X^3 + X^4 + X^5 + X^6$

Properties of Cyclic Codes (1)

Theorem

The nonzero code polynomial of minimum degree in a linear block code is unique.

Proof.

Suppose there are two code polynomials $\mathbf{g}(X)$ and $\mathbf{g}'(X)$ of minimum degree r.

What is the degree of their sum? $\square$

Properties of Cyclic Codes (2)

Let $\mathbf{g}(X) = g_0 + g_1 X + \cdots + g_{r-1} X^{r-1} + X^r$ be the nonzero code polynomial of minimum degree in an (n, k) binary cyclic code C.

Theorem

The constant term g_0 is equal to 1.

Proof.

Suppose $g_0 = 0$.
Then $g_1 X + g_2 X^2 + \cdots + X^r$ is a code polynomial.
What happens when we left shift the corresponding codeword? □

Properties of Cyclic Codes (3)

Let $\mathbf{g}(X) = g_0 + g_1 X + \cdots + g_{r-1} X^{r-1} + X^r$ be the nonzero code polynomial of minimum degree in an (n, k) binary cyclic code C.

Theorem

A binary polynomial of degree $n - 1$ or less is a code polynomial if and only if it is a multiple of $\mathbf{g}(X)$.

Proof.

($\Leftarrow$) A multiple of $\mathbf{g}(X)$ of degree $n - 1$ or less is a linear combination of shifts of $\mathbf{g}(X)$.
($\Rightarrow$) Consider the remainder when a code polynomial is divided by $\mathbf{g}(X)$. $\square$

$\mathbf{g}(X)$ is called the generator polynomial of the cyclic code.

Properties of Cyclic Codes (4)

Theorem

The degree of the generator polynomial of an (n, k) binary cyclic code is $n - k$.

Proof.

If the degree of $\mathbf{g}(X)$ is r, how many distinct multiples of $\mathbf{g}(X)$ of degree of $n - 1$ or less exist? □

Properties of Cyclic Codes (5)

Theorem

The generator polynomial of an (n, k) *binary cyclic code is a factor of* $X^n + 1$*.*

Proof.

$\mathbf{g}(X)$ has degree $n - k$.
What is the remainder when $X^k \mathbf{g}(X)$ is divided by $X^n + 1$? $\square$

Properties of Cyclic Codes (6)

Theorem

If $\mathbf{g}(X)$ is a polynomial of degree $n-k$ and is a factor of X^n+1, then $\mathbf{g}(X)$ generates an (n,k) cyclic code.

Proof.

Multiples of $\mathbf{g}(X)$ of degree $n-1$ or less generate a (n,k) linear block code.
We need to show that the generated code is cyclic.
For a code polynomial $\mathbf{v}(X)$ consider the following equation

$$X\mathbf{v}(X) = v_{n-1}(X^n+1) + \mathbf{v}^{(1)}(X)$$

What can we say about $\mathbf{v}^{(1)}(X)$? □

Systematic Encoding of Cyclic Codes

- To encode a k-bit message $\begin{bmatrix} u_0 & u_1 & \cdots & u_{k-1} \end{bmatrix}$ construct the message polynomial

$$\mathbf{u}(X) = u_0 + u_1 X + \cdots + u_{k-1} X^{k-1}.$$

- Given a generator polynomial $\mathbf{g}(X)$ of an (n, k) cyclic code, the corresponding codeword is $\mathbf{u}(X)\mathbf{g}(X)$. This is not a systematic encoding.
- A systematic encoding of the message can be obtained as follows
    - Divide $X^{n-k}\mathbf{u}(X)$ by $\mathbf{g}(X)$ to obtain remainder $\mathbf{b}(X)$
    - The code polynomial is given by $\mathbf{b}(X) + X^{n-k}\mathbf{u}(X)$

Questions? Takeaways?