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 $\mathbf{v}$

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

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

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

  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 $X^n + 1$
- Polynomial representations of codewords will be called code polynomials

Properties of Cyclic Codes

- The nonzero code polynomial of minimum degree in a linear block code is unique.
- 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) cyclic code C.
  - The constant term g_0 is equal to 1.
  - A binary polynomial of degree $n - 1$ or less is a code polynomial if and only if it is a multiple of $\mathbf{g}(X)$.
  - $\mathbf{g}(X)$ is called the generator polynomial of the cyclic code.
  - The degree of the generator polynomial is $n - k$.
  - The generator polynomial is a factor of $X^n + 1$.
- 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.

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 $\mathbf{b}(X) + X^{n-k}\mathbf{u}$

Questions? Takeaways?