Cyclic Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

August 18, 2015

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 $\mathbf{v}^{(1)}(X)$

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

- 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? $\square$

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? $\square$

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

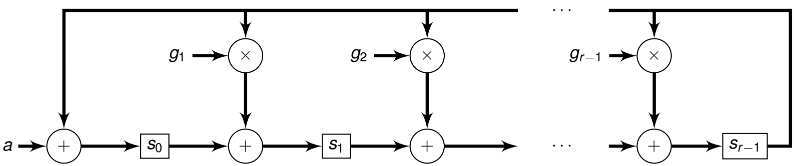
$$\mathbf{u}(X) = u_0 + u_1 X + \cdots + u_{k-1} X^{k-1}.$$

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

Circuits for Cyclic Code Encoding

A Shift Register Circuit

Let $\mathbf{g}(X) = 1 + g_1 X + g_2 X^2 + \cdots + g_{r-1} X^{r-1} + X^r$



$\mathbf{s}(X) = s_0 + s_1 X + \cdots + s_{r-1} X^{r-1}$ is the current state polynomial
The next state polynomial $\mathbf{s}'(X)$ is given by

$$\mathbf{s}'(X) = [a + X\mathbf{s}(X)] \bmod \mathbf{g}(X)$$

Can we use this circuit to build an encoder for a cyclic code with generator polynomial $\mathbf{g}(X)$?

Circuit for Systematic Encoding

- If the initial state polynomial is zero and the input is a sequence of bits $a_{m-1}, a_{m-2}, \ldots, a_1, a_0$, the final state polynomial is

$$\mathbf{a}(X) \bmod \mathbf{g}(X) = \left[\sum_{i=0}^{m-1} a_i X^i\right] \bmod \mathbf{g}(X)$$

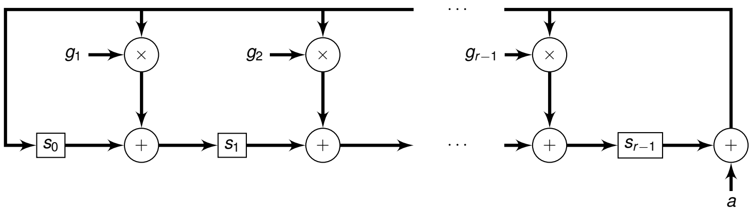
- For systematic encoding we need $X^{n-k}\mathbf{u}(X) \bmod \mathbf{g}(X)$ which corresponds to input bit sequence

$$u_{k-1}, u_{k-2}, \ldots, u_1, u_0, \underbrace{0, 0, \ldots, 0, 0}_{n-k}$$

- Is there a way to avoid the delay of $n-k$ clock ticks?

Another Shift Register Circuit

Let $\mathbf{g}(X) = 1 + g_1 X + g_2 X^2 + \cdots + g_{r-1} X^{r-1} + X^r$



$\mathbf{s}(X) = s_0 + s_1 X + \cdots + s_{r-1} X^{r-1}$ is the current state polynomial
The next state polynomial $\mathbf{s}'(X)$ is given by

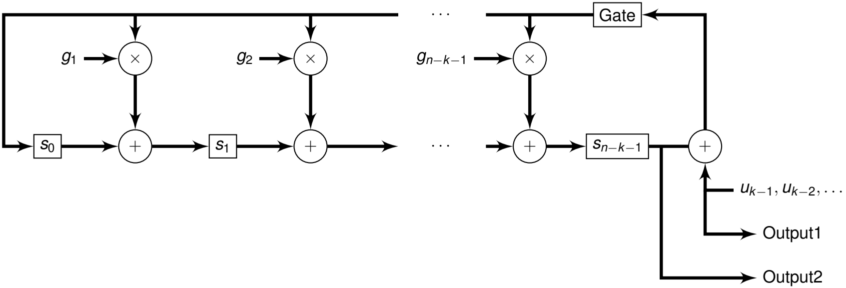
$$\mathbf{s}'(X) = \left[aX^r + X\mathbf{s}(X)\right] \bmod \mathbf{g}(X)$$

If the initial state polynomial is zero and the input is a sequence of bits $a_{m-1}, a_{m-2}, \ldots, a_1, a_0$, the final state polynomial is

$$X^r \mathbf{a}(X) \bmod \mathbf{g}(X) = \left[\sum_{i=0}^{m-1} a_i X^{r+i}\right] \bmod \mathbf{g}(X)$$

Systematic Encoding Circuit for Cyclic Codes

Let $\mathbf{g}(X) = 1 + g_1 X + g_2 X^2 + \cdots + g_{n-k-1} X^{n-k-1} + X^{n-k}$

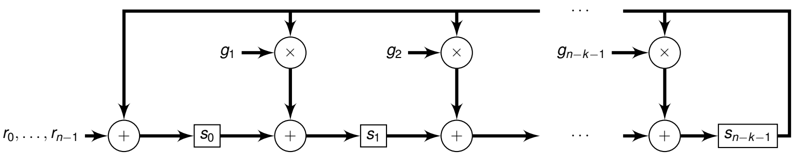


- Turn on the gate. Shift the message bits $u_{k-1}, u_{k-2}, \ldots, u_0$ into the circuit and channel simultaneously. Only Output1 is fed to the channel.
- Turn off the gate and shift the contents of the shift register into the channel. Only Output2 is fed to the channel.

Error Detection using Cyclic Codes

Syndrome Computation

- Errors are detected when the received vector is not a codeword
- For linear block codes, $\mathbf{r}$ is a codeword $\iff \mathbf{r}\mathbf{H}^T = \mathbf{0}$
- $\mathbf{s} = \mathbf{r}\mathbf{H}^T$ is called the syndrome vector
- For cyclic codes, the received polynomial $\mathbf{r}(X)$ is a code polynomial $\iff \mathbf{r}(X) \bmod \mathbf{g}(X) = 0$
- $\mathbf{s}(X) = \mathbf{r}(X) \bmod \mathbf{g}(X)$ is called the syndrome polynomial
- The following circuit computes the syndrome polynomial



Detecting Odd Weight Error Patterns

- For received polynomial $\mathbf{r}(X) = \mathbf{v}(X) + \mathbf{e}(X)$ where $\mathbf{v}(X)$ is a code polynomial

$$\mathbf{r}(X) \bmod \mathbf{g}(X) = \mathbf{e}(X) \bmod \mathbf{g}(X)$$

- Error $\mathbf{e}(X) \neq 0$ is undetected if $\mathbf{e}(X) \bmod \mathbf{g}(X) = 0$
- If an odd weight error pattern occurs, then

$$\mathbf{e}(X) = X^{i_1} + X^{i_2} + \cdots + X^{i_m}$$

  where m is odd and $0 \leq i_j \leq n - 1$
- If $X + 1$ is a factor of $\mathbf{g}(X)$, all odd weight error patterns are detected
- If $\mathbf{g}(X) = (X + 1)\mathbf{a}(X)$, then $\mathbf{e}(X) \bmod \mathbf{g}(X) = 0 \implies \mathbf{e}(X) = \mathbf{g}(X)\mathbf{b}(X) = (X + 1)\mathbf{a}(X)\mathbf{b}(X)$

Detecting Double Bit Errors

- A double bit error pattern is of the form $\mathbf{e}(X) = X^i + X^j$ where $i \neq j$ and $0 \leq i, j \leq n - 1$
- A polynomial over $\mathbb{F}_2$ is said to be irreducible over $\mathbb{F}_2$ if it has no factors other than 1 and itself
  - Examples: $X, X + 1, X^2 + X + 1, X^3 + X + 1, X^3 + X^2 + 1$
- A degree m irreducible polynomial is primitive if the smallest value of N for which it divides $X^N + 1$ is $2^m - 1$
  - Examples: $X + 1, X^2 + X + 1$
- If $\mathbf{g}(X)$ is a primitive polynomial of degree m and the code length $n = 2^m - 1$, then all double bit errors are detected

$$X^i + X^j = X^i(1 + X^{j-i})$$

- In practice, $\mathbf{g}(X)$ is chosen to be $(X + 1)\mathbf{p}(X)$ where $\mathbf{p}(X)$ is a primitive polynomial

Example: CRC-16

- The generator polynomial of CRC-16 is given by

$$\mathbf{g}(X) = X^{16} + X^{15} + X^2 + 1 = (X+1)(X^{15} + X + 1)$$

  CRC = Cyclic Redundancy Check
- All odd weight error patterns are detected
- If the code length is $2^{15} - 1 = 32767$, then all double bit errors are detected
- A burst error of length m occurs if the error locations are confined to a block of length m

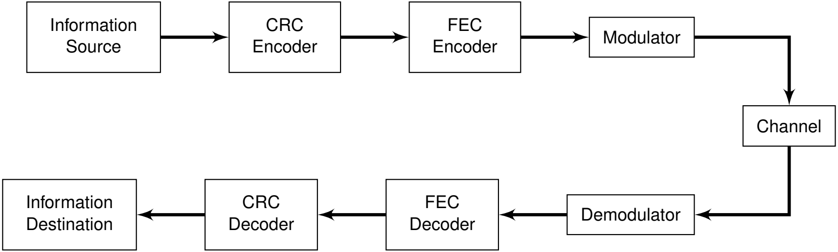
$$e(X) = X^i + e_{i+1}X^{i+1} + e_{i+2}X^{i+2} + \cdots + e_{i+m-2}X^{i+m-2} + X^{i+m-1}$$

- The CRC-16 code can detect all burst errors of length 16 or less

Burst Error Detection

- An (n, k) cyclic code can detect burst errors of length $n - k$ or less, including end-around bursts
- The fraction of undetectable bursts of length $n - k + 1$ is $2^{-(n-k-1)}$
- For $m > n - k + 1$, the fraction of undetectable bursts of length m is $2^{-(n-k)}$

CRC in Context



CRC is used along with Automatic Repeat reQuest (ARQ) to enable reliable communication

Questions? Takeaways?