Modul #10

TE3223
SISTEM KOMUNIKASI 2

CYCLIC BLOCK CODE

Program Studi S1 Teknik Telekomunikasi

Departemen Teknik Elektro - Sekolah Tinggi Teknologi Telkom

Bandung – 2007

Cyclic block codes

- Cyclic codes are a subclass of linear block codes.
- Encoding and syndrome calculation are easily performed using feedback shift-registers.
  - Hence, relatively long block codes can be implemented with a reasonable complexity.
- BCH and Reed-Solomon codes are cyclic codes.

Cyclic block codes

- A linear (n,k) code is called a Cyclic code if all cyclic shifts of a codeword are also a codeword.

$$\mathbf{U} = (u_0, u_1, u_2, \ldots, u_{n-1})$$

"*i*" cyclic shifts of **U**

$$\mathbf{U}^{(i)} = (u_{n-i}, u_{n-i+1}, \ldots, u_{n-1}, u_0, u_1, u_2, \ldots, u_{n-i-1})$$

- Example:

$$\mathbf{U} = (1101)$$

$$\mathbf{U}^{(1)} = (1110) \quad \mathbf{U}^{(2)} = (0111) \quad \mathbf{U}^{(3)} = (1011) \quad \mathbf{U}^{(4)} = (1101) = \mathbf{U}$$

Cyclic block codes

- Algebraic structure of Cyclic codes, implies expressing codewords in polynomial form

$$\mathbf{U}(X) = u_0 + u_1 X + u_2 X^2 + \ldots + u_{n-1} X^{n-1} \qquad \text{degree}\,(n\text{-}1)$$

- Relationship between a codeword and its cyclic shifts:

$$X\mathbf{U}(X) = u_0 X + u_1 X^2 + \ldots, u_{n-2} X^{n-1} + u_{n-1} X^n$$

$$= \underbrace{u_{n-1} + u_0 X + u_1 X^2 + \ldots + u_{n-2} X^{n-1}}_{\mathbf{U}^{(1)}(X)} + \underbrace{u_{n-1} X^n + u_{n-1}}_{u_{n-1}(X^n+1)}$$

$$= \mathbf{U}^{(1)}(X) + u_{n-1}(X^n + 1)$$

  - Hence:

$$\mathbf{U}^{(1)}(X) = X\mathbf{U}(X) \text{ modulo } (X^n + 1)$$

By extension

$$\mathbf{U}^{(i)}(X) = X^i \mathbf{U}(X) \text{ modulo } (X^n + 1)$$

Cyclic block codes

- Basic properties of Cyclic codes:
  - Let C be a binary (n,k) linear cyclic code
    1. Within the set of code polynomials in C, there is a unique monic polynomial $\mathbf{g}(X)$ with minimal degree $r < n$. $\mathbf{g}(X)$ is called the generator polynomials.

       $$\mathbf{g}(X) = g_0 + g_1 X + \ldots + g_r X^r$$

    1. Every code polynomial $\mathbf{U}(X)$ in C, can be expressed uniquely as $\mathbf{U}(X) = \mathbf{m}(X)\mathbf{g}(X)$
    2. The generator polynomial $\mathbf{g}(X)$ is a factor of $X^n + 1$

Cyclic block codes

- The orthogonality of **G** and **H** in polynomial form is expressed as $\mathbf{g}(X)\mathbf{h}(X) = X^n + 1$. This means $\mathbf{h}(X)$ is also a factor of $X^n + 1$

1. The row $i, i = 1,\ldots,k$ of generator matrix is formed by the coefficients of the $"i-1"$ cyclic shift of the generator polynomial.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}(X) \\ X\mathbf{g}(X) \\ \vdots \\ X^{k-1}\mathbf{g}(X) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & & & & \mathbf{0} \\ & g_0 & g_1 & \cdots & g_r & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & g_0 & g_1 & \cdots & g_r & \\ \mathbf{0} & & & & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

Cyclic block codes

- Systematic encoding algorithm for an (n,k) Cyclic code:
  1. Multiply the message polynomial $\mathbf{m}(X)$ by X^{n-k}
  2. Divide the result of Step 1 by the generator polynomial $\mathbf{g}(X)$. Let $\mathbf{p}(X)$ be the reminder.
  3. Add $\mathbf{p}(X)$ to $X^{n-k}\mathbf{m}(X)$ to form the codeword $\mathbf{U}(X)$

Cyclic block codes

- Example: For the systematic (7,4) Cyclic code with generator polynomial $\mathbf{g}(X) = 1 + X + X^3$

1. Find the codeword for the message $\mathbf{m} = (1011)$

$$n = 7,\quad k = 4,\quad n - k = 3$$

$$\mathbf{m} = (1011) \Rightarrow \mathbf{m}(X) = 1 + X^2 + X^3$$

$$X^{n-k}\mathbf{m}(X) = X^3\mathbf{m}(X) = X^3(1 + X^2 + X^3) = X^3 + X^5 + X^6$$

Divide $X^{n-k}\mathbf{m}(X)$ by $\mathbf{g}(X)$:

$$X^3 + X^5 + X^6 = \underbrace{(1 + X + X^2 + X^3)}_{\text{quotient } \mathbf{q}(X)}\underbrace{(1 + X + X^3)}_{\text{generator } \mathbf{g}(X)} + \underbrace{1}_{\text{remainder } \mathbf{p}(X)}$$

Form the codeword polynomial:

$$\mathbf{U}(X) = \mathbf{p}(X) + X^3\mathbf{m}(X) = 1 + X^3 + X^5 + X^6$$

$$\mathbf{U} = (\underbrace{1\ 0\ 0}_{\text{parity bits}}\ \ \underbrace{1\ 0\ 1\ 1}_{\text{message bits}})$$

Cyclic block codes

- Find the generator and parity check matrices, **G** and **H**, respectively.

$$\mathbf{g}(X) = 1 + 1\cdot X + 0\cdot X^2 + 1\cdot X^3 \Rightarrow (g_0, g_1, g_2, g_3) = (1101)$$

$$\mathbf{G} = \left[\begin{array}{ccc:cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

Not in systematic form.
We do the following:

- $\text{row}(1) + \text{row}(3) \rightarrow \text{row}(3)$
- $\text{row}(1) + \text{row}(2) + \text{row}(4) \rightarrow \text{row}(4)$

$$\mathbf{G} = \left[\begin{array}{ccc:cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right] = [\underbrace{\mathbf{P}}\ \underbrace{\mathbf{I}_{4\times 4}}]$$

$$\mathbf{H} = \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = [\underbrace{\mathbf{I}_{3\times 3}}\ \underbrace{\mathbf{P}^T}]$$

Cyclic block codes

- Syndrome decoding for Cyclic codes:
  - Received codeword in polynomial form is given by

$$\mathbf{r}(X) = \mathbf{U}(X) + \mathbf{e}(X)$$

Received codeword ← $\mathbf{r}(X)$; $\mathbf{e}(X)$ → Error pattern

  - The syndrome is the reminder obtained by dividing the received polynomial by the generator polynomial.

$$\mathbf{r}(X) = \mathbf{q}(X)\mathbf{g}(X) + \mathbf{S}(X)$$

$\mathbf{S}(X)$ → **Syndrome**

  - With syndrome and Standard array, error is estimated.
    - In Cyclic codes, the size of standard array is considerably reduced.