Cyclic Codes

Qi Zhang

Aarhus University School of Engieering

17/02, 2014

AARHUS
UNIVERSITET
INGENIØRHØJSKOLEN

Outline

1. Introduction of Cyclic Code
2. Polynomial Representation of Codewords
3. Generator Polynomial of a Cyclic Code
4. Cyclic Codes in Systematic Form
5. Generator Matrix of a Cyclic Code
6. Syndrome Calculation and Error Detection
7. Decoding of Cyclic Codes
8. Burst Error Detection Capability
9. An Cyclic codes application example

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Introduction of cyclic code

- For a given vector of n components, $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$, a right-shift of its components generates a different vector.
- Right shift the original vector for i times, the new vector is

$$\mathbf{c}^{(i)} = (c_{n-i}, c_{n-i+1}, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{n-i-1})$$

- **Cyclic code**: If each code vector of a given linear block code right-shift i times and it becomes another vector of the same code, then this code is a cyclic code.
- As cyclic code is a class of linear block code, the sum of two cyclic code vectors is also a code vector of this cyclic code.

An example of cyclic code

Code vector **c**						
0	0	0	0	0	0	0
1	0	1	0	0	0	1
1	1	1	0	0	1	0
0	1	0	0	0	1	1
0	1	1	0	1	0	0
1	1	0	0	1	0	1
1	0	0	0	1	1	0
0	0	1	0	1	1	1
1	1	0	1	0	0	0
0	1	1	1	0	0	1
0	0	1	1	0	1	0
1	0	0	1	0	1	1
1	0	1	1	1	0	0
0	0	0	1	1	0	1
0	1	0	1	1	1	0
1	1	1	1	1	1	1

Polynomial representation codewords

- Codewords of a given cyclic code $C_{cyc}(n, k)$ can be represented by polynomials.
- A polynomial representation $c(X)$ of a code vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$:

$$c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \qquad c_i \in GF(2^m)$$

  - The polynomial is an expression of a variable X and consists of terms in the form of $c_i X^i$;
  - The coefficients c_i are defined over GF(2^m);
  - Exponent i is an integer number that corresponds to the position of the coefficient or element in a given code vector.
  - If $c_{n-1} = 1$, the polynomial is called *monic*.
  - A code vector of n components is represented by a polynomial of degree $n - 1$ or less.
  - Codewords of a given $C_{cyc}(n, k)$ can be equivalently referred to as code vectors or code polynomials.

Polynomial representation codewords

- Operation of two polynomials, whose coefficients are defined over GF(2):

$$\begin{aligned} c_1(X) &= c_{01} + c_{11}X + \ldots + c_{n-1,1}X^{n-1} \\ c_2(X) &= c_{02} + c_{12}X + \ldots + c_{n-1,2}X^{n-1} \end{aligned}$$

  - Addition:

$$c_1(X) \oplus c_2(X) = (c_{01} \oplus c_{02}) + (c_{11} \oplus c_{12})X + \ldots + (c_{n-1,1} \oplus c_{n-1,2})X^{n-1}$$

  - Multiplication:

$$\begin{aligned} c_1(X) \bullet c_2(X) &= (c_{01} \bullet c_{02}) + (c_{01} \bullet c_{12} \oplus c_{11} \bullet c_{02})X + \ldots \\ &\quad + (c_{n-1,1} \bullet c_{n-1,2})X^{2(n-1)} \end{aligned}$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Polynomial representation codewords

- **Example**: Two polynomials $c_1(X)$ and $c_2(X)$ defined over GF(2).

$$\begin{aligned} c_1(X) &= 1 + X \\ c_2(X) &= 1 + X + X^2 \end{aligned}$$

Calculate $c_1(X) + c_2(X)$, $c_1(X) \bullet c_2(X)$.

- **Solution**:

$$c_1(X) + c_2(X) = (1 + X) + (1 + X + X^2) = X^2$$

$$c_1(X) \bullet c_2(X) = (1+X)(1+X+X^2) = 1+X+X^2+X+X^2+X^3 = 1+X^3$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Polynomial representation codewords

- Division of polynomials.
- Let $c_1(X)$ and $c_2(X)$ two polynomials defined over GF(2). And $c_2(X) \neq 0$, a non-zero polynomial.
- The division between $c_1(X)$ and $c_2(X)$ can be written as

$$c_1(X) = q(X) \bullet c_2(X) \oplus r(X)$$

  - $q(X)$ is the quotient.
  - $r(X)$ is the remainder.

Polynomial representation codewords

- **Example**: Two polynomials $c_1(X)$ and $c_2(X)$ defined over GF(2).

$$\begin{aligned} c_1(X) &= 1 + X^3 \\ c_2(X) &= 1 + X \end{aligned}$$

  Calculate $c_1(X)/c_2(X)$.

- $$c_1(X)/c_2(X) = 1 + X + X^2$$

Generator polynomial of a cyclic code

$$\begin{aligned} \mathbf{c} &= (c_0, c_1, \ldots, c_{n-1}) \\ c(X) &= c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \end{aligned}$$

- After i-position right-shift, there is

$$\begin{aligned} \mathbf{c}^{(i)} &= (c_{n-i}, c_{n-i+1}, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{n-i-1}) \\ &\Downarrow \\ c^{(i)}(X) &= c_{n-i} + c_{n-i+1} X, + \ldots + c_{n-i-1} X^{n-1} \end{aligned}$$

- $c^{(i)}(X)$ is the remainder of the division of $X^i c(X)$ and $(X^n + 1)$:

$$\begin{aligned} X^i c(X) &= q(X)(X^n + 1) + c^{(i)}(X) \\ c^{(i)}(X) &= X^i c(X) \bmod (X^n + 1) \end{aligned}$$

Generator polynomial of a cyclic code

- **Example**: A codeword of Cyclic code $C_{cyc}(7,4)$, $\mathbf{c} = (0\ 1\ 1\ 0\ 1\ 0\ 0)$, right shift 3 times. To verify $c^{(3)}(X) = X^3 c(X) \bmod (X^7+1)$
- **Solution**:

$$\begin{aligned} \mathbf{c} &= (0\ 1\ 1\ 0\ 1\ 0\ 0) \\ &\Downarrow \\ \mathbf{c}^{(3)} &= (1\ 0\ 0\ 0\ 1\ 1\ 0) \\ c^{(3)}(X) &= 1 + X^4 + X^5 \end{aligned}$$

$$\begin{aligned} c(X) &= X + X^2 + X^4 \\ X^3 c(X) \bmod (X^7+1) &= X^3(X + X^2 + X^4) \bmod (X^7+1) \\ &= 1 + X^4 + X^5 \\ &= c^{(3)}(X) \end{aligned}$$

Generator Polynomial of a Cyclic Code

- Assuming polynomial $g(X) = g_0 + g_1 X + \ldots + X^r$ has the minimum degree among all the code polynomials of a given code $C_{cyc}(n,k)$.
- The non-zero minimum-degree code polynomial of a given cyclic code $C_{cyc}(n,k)$ is unique.
  - If there is another polynomial $g_1(X) = g_{01} + g_{11} X + \ldots + X^r$;
  - As cyclic code is linear block code, the sum of two code polynomials is another code polynomial;
  - Assuming $g_2(X) = g(X) + g_1(X)$, thus the coefficient of the item X^r in $g_2(X)$ is 0;
  - It contradicts with the original statement that $g(X)$ has the minimum degree
- Therefore, the non-zero minimum-degree code polynomial of a given cyclic code $C_{cyc}(n,k)$ is unique.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Generator Polynomial of a Cyclic Code

- **THEOREM**: Let $g(X) = g_0 + g_1 X + \ldots + g_{r-1} X^{r-1} + X^r$ be the non-zero minimum degree code polynomial of a cyclic code $C_{cyc}(n, k)$, then the constant term g_0 must equal to 1.
- Proof:
  - Suppose that $g_0 = 0$. Then $g(X) = g_1 X + \ldots + g_{r-1} X^{r-1} + X^r$
  - If we shift $g(X)$ cyclically $n - 1$ positions to the right (or one position to the left), we obtain a non-zero code polynomial: $g_1 + \ldots + g_{r-1} X^{r-2} + X^{r-1}$.
  - The new polynomial is of degree less than r. This is contradiction to the assumption that $g(X)$ is non-zero code polynomial with minimum degree. Thus, $g_0 \neq 0$.
- Therefore, the non-zero minimum degree code polynomial of a given cyclic code $C_{cyc}(n, k)$ is

$$g(X) = 1 + g_1 X + \ldots + g_{r-1} X^{r-1} + X^r$$

Generator Polynomial of a Cyclic Code

- As we know

$$g(X) = 1 + g_1 X + \ldots + g_{r-1} X^{r-1} + X^r$$

$$\begin{aligned} Xg(X) &= g^{(1)}(X) \\ X^2 g(X) &= g^{(2)}(X) \\ &\vdots \\ X^{n-r-1} g(X) &= g^{(n-r-1)}(X) \end{aligned}$$

- The degrees of all these polynomials $Xg(X), X^2g(X), \ldots, X^{n-r-1}g(X)$ are less than n. Therefore, these polynomials are the remainder polynomials if divided by $X^n + 1$.
- $Xg(X), X^2g(X), \ldots, X^{n-r-1}g(X)$ are the right-shift rotation of $g(X)$.
- They are code polynomials, based on cyclic code definition.

Generator Polynomial of a Cyclic Code

- Since cyclic code is also linear block code, linear combination of code polynomials is also a code polynomial, therefore,

$$\begin{aligned} c(X) &= m_0 g(X) + m_1 g^{(1)}(X) + \ldots + m_{n-r-1} g^{(n-r-1)}(X) \\ &= m_0 g(X) + m_1 X g(X) + \ldots + m_{n-r-1} X^{n-r-1} g(X) \\ &= (m_0 + m_1 X + \ldots + m_{n-r-1} X^{n-r-1}) g(X) \\ &= m(X) g(X) \end{aligned}$$

- **It means a code polynomial $c(X)$ is a multiple of the non-zero minimum-degree polynomial $g(X)$.**

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Generator Polynomial of a Cyclic Code

- We know $c(X) = (m_0 + m_1 X + \ldots + m_{n-r-1} X^{n-r-1}) g(X) = m(X) g(X)$
  - m_i is defined over GF(2), i.e, m_i is equal to 1 or 0.
  - Polynomial, $m(X) = (m_0 + m_1 X + \ldots + m_{n-r-1} X^{n-r-1})$, consists of $n - r$ terms. Therefore, there are 2^{n-r} different polynomials $m(X)$.
  - In other words, based on $g(X)$, it can form 2^{n-r} different polynomials $c(X)$ with degree $n - 1$ or less.
- If rewrite $n - r = k$ and $r = n - k$, $c(X)$ can be regarded as the code polynomial of $C_{cyc}(n, k)$.
- So $m(X)$ can be regarded as message polynomial, m_i, $i = 0, 1, \ldots k - 1$, are the bits of message vector.
- In a cyclic code $C_{cyc}(n, k)$ there is a unique non-zero minimum-degree code polynomial, and any other polynomial is a multiple of this polynomial.
- The non-zero minimum-degree code polynomial completely determines and generates the cyclic code. It is called **generator polynomial**.

An example of cyclic code $C_{cyc}(7,4)$

Code vector $\mathbf{c}$						
0	0	0	0	0	0	0
1	0	1	0	0	0	1
1	1	1	0	0	1	0
0	1	0	0	0	1	1
0	1	1	0	1	0	0
1	1	0	0	1	0	1
1	0	0	0	1	1	0
0	0	1	0	1	1	1
1	1	0	1	0	0	0
0	1	1	1	0	0	1
0	0	1	1	0	1	0
1	0	0	1	0	1	1
1	0	1	1	1	0	0
0	0	0	1	1	0	1
0	1	0	1	1	1	0
1	1	1	1	1	1	1

An example of cyclic code $C_{cyc}(7,4)$

Code vector **c**						
0	0	0	0	0	0	0
1	0	1	0	0	0	1
1	1	1	0	0	1	0
0	1	0	0	0	1	1
0	1	1	0	1	0	0
1	1	0	0	1	0	1
1	0	0	0	1	1	0
0	0	1	0	1	1	1
1	1	0	1	0	0	0
0	1	1	1	0	0	1
0	0	1	1	0	1	0
1	0	0	1	0	1	1
1	0	1	1	1	0	0
0	0	0	1	1	0	1
0	1	0	1	1	1	0
1	1	1	1	1	1	1

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Generator Polynomial of a Cyclic Code

- **Property**:
  - if $g(X)$ is a generator polynomial of a given linear cyclic code $C_{cyc}(n, k)$, then $g(X)$ is a factor of $X^n + 1$.
  - if a polynomial of degree $r = n - k$ is a factor of $X^n + 1$, then this polynomial generates a linear cyclic code $C_{cyc}(n, k)$.

Generator Polynomial of a Cyclic Code

- **Example 3.1**: Determine the code vectors corresponding to the message vectors of the linear cyclic code $C_{cyc}(7,4)$ generated by the generator polynomial $g(X) = 1 + X + X^3$.

$$\mathbf{m}_0 = (0000) \quad \mathbf{m}_1 = (1000) \quad \mathbf{m}_2 = (0100) \quad \mathbf{m}_3 = (1100) \quad \mathbf{m}_4 = (1010)$$

Message **m**	$m(X)$	Code polynomial	Code vector **c**
0000	0	$0g(X) = 0$	0000000
1000	1	$1g(X) = 1 + X + X^3$	1101000
0100	X	$Xg(X) = X + X^2 + X^4$	0110100
1100	$1 + X$	$(1 + X)g(X) = 1 + X^2 + X^3 + X^4$	1011100
1010	$1 + X^2$	$(1 + X^2)g(X) = 1 + X + X^2 + X^5$	1110010

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Cyclic codes in systematic form

- Previously, encoding procedure is based on $c(X) = m(X)g(X)$.
- However, the generated codes is non-systematic.

Cyclic codes in systematic form

- To generate systematic cyclic code, follow the following steps:
  - Form polynomial $X^{n-k}m(X)$;
  - Divide $X^{n-k}m(X)$ by generator polynomial $g(X)$. $p(X)$ is the remainder polynomial here.

$$X^{n-k}m(X) = q(X)g(X) + p(X)$$

  - Rewrite the above equation into:

$$q(X)g(X) = X^{n-k}m(X) + p(X)$$

  - We can see $q(X)g(X)$ is a code polynomial, as it is a multiple of $g(X)$.
  - The term $X^{n-k}m(X)$ represents the message polynomial right shift $n-k$ positions.
  - The remainder polynomial $p(X)$ works as redundancy polynomial.
  - So $X^{n-k}m(X) + p(X)$ gives the systematic form of the code polynomial.

Cyclic codes in systematic form

- The systematic form of the code polynomial:

$$\begin{aligned} c(X) &= X^{n-k} m(X) + p(X) \\ &= p_0 + p_1 X + \ldots + p_{n-k-1} X^{n-k-1} + m_0 X^{n-k} + m_1 X^{n-k+1} + \ldots + m_{k-1} X^{n-1} \end{aligned}$$

- Code vector can be expressed based on code polynomial as:

$$\mathbf{c} = (p_0, p_1, \ldots, p_{n-k-1}, m_0, m_1, \ldots, m_{k-1})$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Encoding of cyclic codes in systematic form

- **Summary** Encoding of a cyclic codes $C_{cyc}(n, k)$ in systematic form consists three steps:
  1. Multiplying the message polynomial $m(X)$ by X^{n-k}, forming $X^{n-k}m(X)$;
  2. Diving $X^{n-k}m(X)$ by $g(X)$, obtaining the remained polynomial $p(X)$;
  3. Forming the code polynomial $c(X) = p(X) + X^{n-k}m(X)$.

Cyclic codes in systematic form

- **Example 3.2**: For the cyclic code $C_{cyc}(7,4)$ generated by $g(X) = 1 + X + X^3$, determine the systematic form of the codeword corresponding to the message vector $\mathbf{m} = (1010)$.
- **Solution**:
  - Form polynomial $X^{n-k}m(X) = X^{7-4}(1 + X^2) = X^3 + X^5$;
  - Divide $X^3 + X^5$ by $g(X)$, obtain $p(X) = X^2$;
  - $c(X) = X^{n-k}m(X) + p(X) = X^2 + X^3 + X^5$;
  - $\mathbf{c} = (0011010)$.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Generator matrix of a cyclic code

$$g(X) = 1 + g_1 X + \ldots + g_{n-k-1} X^{n-k-1} + X^{n-k}$$

- Span the generator polynomial by k code polynomials, $g(X), Xg(X), \ldots, X^{k-1}g(X)$,
- Represent each above code polynomial by code vector and use as a row in the matrix,
- A matrix of dimension $k \times n$ is formed:

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & & \vdots \\ 0 & 0 & & \cdots & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{bmatrix}$$

where $g_0 = g_{n-k} = 1$.

- A systematic form generator matrix can always be obtained by row operations of the non-systematic generator matrix.

Generator matrix of a cyclic code

- **Example 3.3**: For the linear cyclic code $C_{cyc}(7,4)$ generated by polynomial $g(X) = 1 + X + X^3$, determine the corresponding generator matrix and convert it into a systematic form.
- **Solution**:
  - According to $g(X)$, there is $\mathbf{g}_0 = (g_0, g_1, g_2, g_3, g_4, g_5, g_6) = (1101000)$.
  - So generator matrix $\mathbf{G}$ of dimension $k \times n = 4 \times 7$ can be expressed by

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \\ \mathbf{g}_3 \end{bmatrix}$$

  - By row operation: $\mathbf{g}_2 = \mathbf{g}_0 \oplus \mathbf{g}_2$ and $\mathbf{g}_3 = \mathbf{g}_0 \oplus \mathbf{g}_1 \oplus \mathbf{g}_3$, a generator matrix in systematic form is obtained:

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

Generator matrix of a cyclic code

- **Example 3.4**: The polynomial $X^7 + 1$ can be factorized as follows:

  $$X^7 + 1 = (1 + X)(1 + X + X^3)(1 + X^2 + X^3)$$

  How many different cyclic codes of length 7 can be generated?

- **Solution**: There are six different cyclic codes of length 7, as we can find six different generator polynomials that are the factors of $X^7 + 1$.

Generator polynomial	Codes
$g_1 = (1 + X)$	$C_{cyc}(7, 6)$
$g_2 = (1 + X + X^3)$	$C_{cyc}(7, 4)$
$g_3 = (1 + X^2 + X^3)$	$C_{cyc}(7, 4)$
$g_4 = (1 + X)(1 + X + X^3)$	$C_{cyc}(7, 3)$
$g_5 = (1 + X)(1 + X^2 + X^3)$	$C_{cyc}(7, 3)$
$g_6 = (1 + X + X^3)(1 + X^2 + X^3)$	$C_{cyc}(7, 1)$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Syndrome calculation

- Suppose the receive vector and receive polynomial are

$$\begin{aligned}\mathbf{r} &= (r_0, r_1, r_2, \ldots, r_{n-1}) \\ r(X) &= r_0 + r_1X + r_2X^2 \ldots + r_{n-1}X^{n-1}\end{aligned}$$

- Divide $r(X)$ by generator polynomial $g(X)$:

$$r(X) = q(X)g(X) + S(X)$$

  - $S(X)$ is remainder, of degree $n-k-1$ or less;
  - $q(X)g(X)$ is a code polynomial;
  - If $S(X) = 0$, then $r(X)$ is a code polynomial; otherwise, error is detected.
  - Therefore, $S(X)$ is the syndrome polynomial, $S(X) = s_0 + s_1X + \ldots + s_{n-k-1}X^{n-k-1}$.

Error polynomial and Syndrome calculation

- We know $r(X) = q(X)g(X) + S(X)$.
- We can also write $r(X) = c(X) + e(X)$.
- Rewrite the expression to:

$$\begin{aligned} e(X) &= c(X) + r(X) \\ &= c(X) + q(X)g(X) + S(X) \\ &= (f(X) + q(X))g(X) + S(X) \end{aligned}$$

- If error polynomial $e(X)$ is divided by generator polynomial $g(X)$, the remainder is the syndrome polynomial $S(X)$.

Basic decoding of cyclic codes

- Decoding of cyclic codes as a basic linear block code consists of three steps:
  1. Construct error pattern and syndrome vector lookup table.
  2. Syndrome calculation based on received polynomial.
  3. Error correction by adding error polynomial and received polynomial.

Basic decoding of cyclic codes

- **Example 3.5**: $C_{cyc}(7,4)$ generated by $g(X) = 1 + X + X^3$, which has minimum Hamming distance $d_{min} = 3$, can correct any single error pattern. Construct error pattern and syndrome vector lookup table. Decode $\mathbf{r} = (1011011)$.
- **Solution part I**:
  - There are seven single error patterns.
  - Syndrome polynomial can be calculated by $S(X) = e(X) \; mod \; g(X)$.

Error pattern and syndrome vector lookup table:

Error pattern	Syndrome polynomial	Syndrome vector
$e_6(X) = X^6$	$S(X) = 1 + X^2$	1 0 1
$e_5(X) = X^5$	$S(X) = 1 + X + X^2$	1 1 1
$e_4(X) = X^4$	$S(X) = X + X^2$	0 1 1
$e_3(X) = X^3$	$S(X) = 1 + X$	1 1 0
$e_2(X) = X^2$	$S(X) = X^2$	0 0 1
$e_1(X) = X^1$	$S(X) = X$	0 1 0
$e_0(X) = X^0$	$S(X) = 1$	1 0 0

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Basic decoding of cyclic codes

- **Example 3.5**: $C_{cyc}(7,4)$ generated by $g(X) = 1 + X + X^3$, which has minimum Hamming distance $d_{min} = 3$, can correct any single error pattern. Construct error pattern and syndrome vector lookup table. Decode $\mathbf{r} = (1011011)$.

Error pattern	Syndrome polynomial	Syndrome vector
$e_6(X) = X^6$	$S(X) = 1 + X^2$	1 0 1
$e_5(X) = X^5$	$S(X) = 1 + X + X^2$	1 1 1
$e_4(X) = X^4$	$S(X) = X + X^2$	0 1 1
$e_3(X) = X^3$	$S(X) = 1 + X$	1 1 0
$e_2(X) = X^2$	$S(X) = X^2$	0 0 1
$e_1(X) = X^1$	$S(X) = X$	0 1 0
$e_0(X) = X^0$	$S(X) = 1$	1 0 0

- **Solution part II**:
  - Since $S(X) = r(X)\ (mod)\ g(X)$, obtain $S(X) = X^2$.
  - Looking up in the above table, notice that $e(X) = X^2$,
  - Combining **e** and **r**, obtain $\mathbf{c} = (1001011)$

Decoding of cyclic codes

- The limitation of the previous approach is that the complexity of the decoding circuit tends to grow exponentially with the code length and with the number of errors that are going to be corrected.
- Cyclic codes have considerable algebraic and geometric properties. If these properties are properly used, decoding circuit can be simplied.

THEOREM 3.1

- **THEOREM 3.1**: If the received polynomial $r(x) = r_0 + r_1X + r_2X^2 \ldots + r_{n-1}X^{n-1}$ generates the syndrome polynomial $S(X)$.Then a cyclic right shift of the received polynomial $r^{(1)}(X)$ generates the syndrome polynomial $S^{(1)}(X)$. $S^{(1)}(X)$ actually is the remainer of diving $XS(X)$ by generator polynomial $g(X)$.

$$\begin{tikzcd}
r(X) \arrow[r, Rightarrow, "rightshift"] \arrow[d, Rightarrow] & r^{(1)}(X) \arrow[d, Rightarrow] \\
S(X) \arrow[r, phantom, "?"] & S^{(1)}(X)
\end{tikzcd}$$

- $S^{(1)}(X) = XS(X)\ mod\ g(X)$

THEOREM 3.1

- **THEOREM 3.1**: If the received polynomial $r(x) = r_0 + r_1X + r_2X^2 \ldots + r_{n-1}X^{n-1}$ generates the syndrome polynomial $S(X)$. Then a cyclic right shift of the received polynomial $r^{(1)}(X)$ generates the syndrome polynomial $S^{(1)}(X)$. $S^{(1)}(X)$ actually is the remainer of diving $XS(X)$ by generator polynomial $g(X)$.
- Proof:
  - There is $Xr(X) = r_{n-1}(X^n + 1) + r^{(1)}(X)$ or $r^{(1)}(X) = r_{n-1}(X^n + 1) + Xr(X)$.
  - The above expression is divided by $g(X)$,

$$f(X)g(X) + t(X) = r_{n-1}g(X)h(X) + X[q(X)g(X) + S(X)]$$

  - As $t(X)$ is the remainder resulting from diving $r^{(1)}(X)$ by $g(X)$, $t(X)$ is the syndrome of $r^{(1)}(X)$.
  - Reordering the equation, there is $XS(X) = [f(X) + r_{n-1}h(X) + Xq(X)]g(X) + t(X)$.
  - We see $t(X) = XS(X)\ mod\ g(X)$. Hence, $t(X) = S^{(1)}(X)$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

An example of using THEOREM 3.1

- A cyclic code $C_{cyc}(7,4)$ is generated by $g(X) = 1 + X + X^3$. Suppose that the received vector is $\mathbf{r} = (0010110)$ and the syndrome of $\mathbf{r}$ is $\mathbf{s} = (101)$. If right shift $\mathbf{r}$ once, the syndrome of $\mathbf{r}^{(1)} = (0001011)$, $\mathbf{s}^{(1)} = (100)$.
- $S^{(1)}(X) = XS(X)\ mod\ g(X) = (X^3 + X)\ mod\ g(X) = 1$

THEOREM 3.1

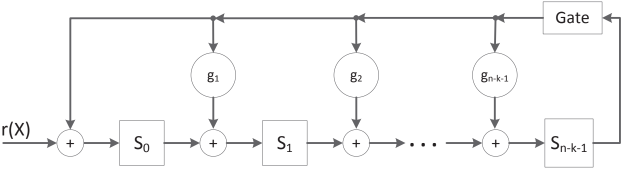
- Following Theorem 3.1 that remainder $S^{(i)}(X)$ resulting from diving $X^i S(X)$ by generator polynomial $g(X)$ is the syndrome polynomial of $r^{(i)}(X)$.
- Theorem 3.1 is the basis of Meggitt Decoding.

Syndrome Circuit

- We have known syndrome polynomial $S(X)$ is the remainer of dividing $r(X)$ by $g(X)$, i.e.,

$$r(X) = q(X)g(X) + s(X)$$

- $S(X)$ is a polynomial of degree $n - k - 1$ or less.
- The syndrome can be computed with a division circuit shown below:



- With all coefficients of **s**, i.e. s_0, s_1, s_{n-k-1} initially set to 0, the $r(X)$ is shifted into the register.
- As soon as the entire $r(X)$ has been shifted into the register, the contents in the register form the syndrome **s**.

Syndrome Circuit for $C_{cyc}(7,4)$ generated by $g(X) = 1 + X + X^3$

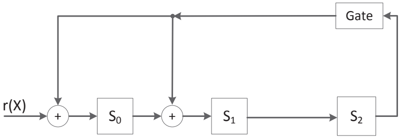


Table: Content of the syndrome register with $\mathbf{r} = (0010110)$

Shift	Input	Register contents
		0 0 0 (initial state)
1	0	0 0 0
2	1	1 0 0
3	1	1 1 0
4	0	0 1 1
5	1	0 1 1
6	0	1 1 1
7	0	1 0 1 (syndrome $\mathbf{s}$)
8	-	1 0 0 (syndrome $\mathbf{s}^{(1)}$)
9	-	0 1 0 (syndrome $\mathbf{s}^{(2)}$)

- THEOREM 3.1 is useful, because shifting the syndrome register once with $S(X)$ as the initial contents is equivalent to obtaining the remainer of dividing $XS(X)$ by $g(X)$. Namely, after one shift, the syndrome register contains $S^{(1)}(X)$.
- Thus to obtain the syndrome $S^{(i)}(X)$ of $r^{(i)}(X)$, we simply shift the syndrome register i times with $S(X)$ as the initial contents.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Decoding of cyclic codes: Meggitt Decoding

- The cyclic structure of a cyclic code allows us to decode a received polynomial $r(X) = r_0 + r_1X + r_2X^2 + ... + r_{n-1}X^{n-1}$ serially, i.e, the received digits are decoded one at a time and each digit is decoded with the same circuitry.
- As soon as the syndrome has been computed, the decoding circuit checks whether the current syndrome S(X) corresponds to a correctable error pattern $e(X) = e_0 + e_1X + \ldots + e_{n-1}X^{n-1}$ with an error at the highest-order postion X^{n-1} (i.e., $e_{n-1} = 1$).
- If $S(X)$ does not corresponds to an error pattern with $e_{n-1} = 1$, then
  - right shift $r(X)$ once. Thus we have $r^{(1)}(X) = r_{n-1} + r_0X + r_1X^2 + ... + r_{n-2}X^{n-1}$.
  - The same decoding circuit will check if $S^{(1)}(X)$ corresponds to an error pattern with an error at location X^{n-1}.

Decoding of cyclic codes: Meggitt Decoding

continuing

- If $S(X)$ of $r(X)$ does corresponds to an error pattern $e(X) = e_0 + e_1 X + \ldots + e_{n-1} X^{n-1}$ with an error at the highest-order position X^{n-1} (i.e., $e_{n-1} = 1$)
  - r_{n-1} is an erroneous digit and it must be corrected.
  - The correction is done by sum $r_{n-1} \oplus 1$. And the correction results in a modified received polynomial $r_1(X) = r_0 + r_1 X + r_2 X^2 + \ldots + (r_{n-1} \oplus 1) X^{n-1}$.

$$\begin{aligned}
r_1(X) &= r(X) + X^{n-1} = [q(X)g(X) + S(X)] + X^{n-1} \\
S_1(X) &= S(X) + X^{n-1} \\
r_1(X) &\Rightarrow^{shift} r_1^{(1)}(X) \\
S_1(X) &\Rightarrow^{shift} S_1^{(1)}(X) = XS_1(X) \ mod \ g(X) \\
XS_1(X) &= XS(X) + (X^n + 1) + 1 \\
&= h(X)g(X) + S^{(1)}(X) + f(X)g(X) + 1 \\
&= (h(X) + f(X))g(X) + S^{(1)}(X) + 1
\end{aligned}$$

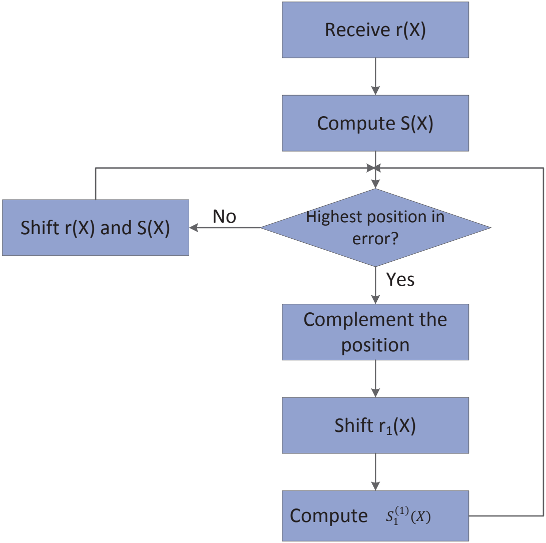
  - Hence, $S_1^{(1)}(X) = S^{(1)}(X) + 1$

Decoding of cyclic codes: Meggitt Decoding

continue...

- The decoding circuitry proceeds to decode the received digit r_{n-2}.
- The decoding of r_{n-2} and the other received digits is identical to the decoding of r_{n-1}.
- Whenever an error is detected and corrected, its effect on the syndrome is removed.
- The decoding stops after a total of n shifts.
- If $e(X)$ is a corretable error pattern, the content in the syndrome register in the end should be zero.
- If the syndrome register does not contain all zeros at the end of decoding process, an uncorretable error pattern has been detected.

Flow Chart of Meggitt Decodign



Block diagram of Meggitt Decoder

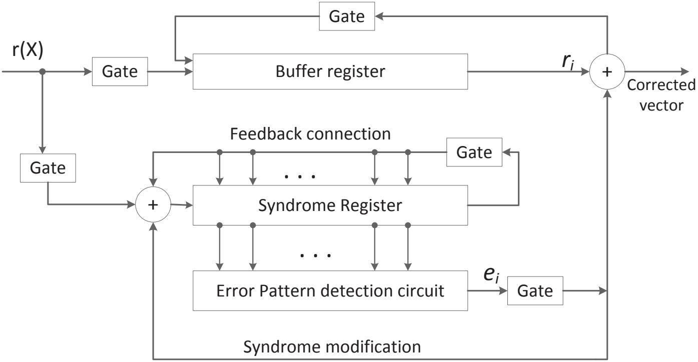
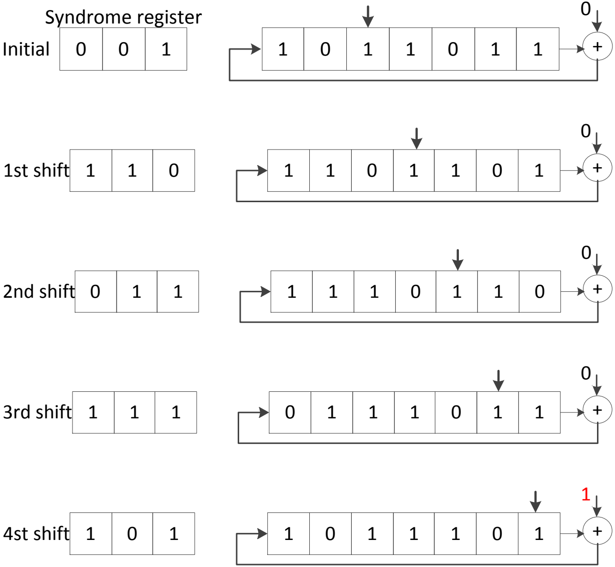


Figure: General cyclic code decoder with received polynomial $r(X)$ shifted into the syndrome register from the left end.

Decoding of cyclic codes: Meggitt Decoding

- Consider the decoding of the $C_{cyc}(7,4)$ generated by $g(X) = 1 + X + X^3$. The error pattern of e_6 has syndrome vector $\mathbf{s} = (101)$.

Decoding of cyclic codes: Meggitt Decoding

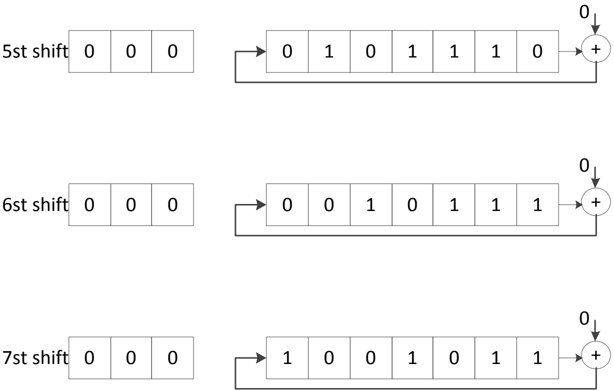


Syndrome register

Initial	0	0	1	1	0	1	1	0	1	1	0
1st shift	1	1	0	1	1	0	1	1	0	1	0
2nd shift	0	1	1	1	1	1	0	1	1	0	0
3rd shift	1	1	1	0	1	1	1	0	1	1	0
4st shift	1	0	1	1	0	1	1	1	0	1	1

Decoding of cyclic codes: Meggitt Decoding

continue...



5st shift 0 0 0 0 1 0 1 1 1 0 + 0

6st shift 0 0 0 0 0 1 0 1 1 1 + 0

7st shift 0 0 0 1 0 0 1 0 1 1 + 0

Burst Error Detection Capability

$$r(X) = c(X) + e(X) = q(X)g(X) + S(X)$$
$$e(X) = c(X) + q(X)g(X) + S(X) = (f(X) + q(X))g(X) + S(X)$$

- Investigate error detecting capability of cyclic code:
  - Assuming $e(X)$ is a burst of length $n-k$ or less, i.e., errors are confined to $n-k$ or fewer consecutive positions;
  - $e(X)$ can be expressed by $e(X) = X^j B(X)$, here $B(X)$ is a polynomial of degree $n-k-1$ or less;
  - X^j cannot divided by $g(X)$, $B(X)$ cannot divided by $g(X)$ neither, $e(X) = X^j B(X)$ is NOT divisible by $g(X)$;
  - Thus the syndrome polynomial is not equal to zero.
  - **It means that a cyclic code $C_{cyc}(n, k)$ can detect any error burst of length $n-k$ or less.**
  - A cyclic code $C_{cyc}(n, k)$ can also detect all the *end-around* error bursts of length $n-k$ or less.

$$\begin{array}{ccccccccccccc} e & = & (1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1) \\ & & \leftarrow & \hookleftarrow & & & & & & & \hookrightarrow & \rightarrow & \rightarrow \end{array}$$

Burst Error Detection Capability

- **Q**: Can a cyclic code detect error-bursts of length $n-k+1$ or longer?
- First, look at error bursts of length of $n-k+1$.
  - Consider the burst of length $n-k+1$ starting from position i and ending at position $i+n-k$.
  - In such error bursts errors are confined to digits $e_i, e_{i+1}, \ldots, e_{i+n-k}$ with $e_i = e_{i+n-k} = 1$.
  - We can see that there are 2^{n-k-1} such bursts.
  - Among these bursts, the only one that cannot be detected is

$$e(X) = X^i g(X)$$

  - So the fraction of undetectable burst of length $n-k+1$ is $1/2^{n-k-1}$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Burst Error Detection Capability

- **Q**: Can a cyclic code detect error-bursts of length $n - k + 1$ or longer?
- Second, look at error bursts of length of $n - k + 1$.
  - Consider the burst of length $l > n - k + 1$ starting from position i and ending at position $i + l - 1$.
  - In such error bursts errors are confined to digits $e_i, e_{i+1}, \ldots, e_{i+l-1}$ with $e_i = e_{i+l-1} = 1$.
  - We can see that there are 2^{l-2} such bursts.
  - Among these bursts, the undetectable ones must following the form:

$$e(X) = X^i a(X) g(X)$$

    - where $a(X) = a_0 + a_1 X + \ldots + a_{l-(n-k)-1} X^{l-(n-k)-1}$ with $a_0 = a_{l-(n-k)-1} = 1$,
    - the number of such bursts is $2^{l-(n-k)-2}$.
  - So the fraction of undetectable burst of length l is $2^{l-(n-k)-2}/2^{l-2} = 1/2^{n-k}$

Error detection summary

- **Theorem**: A cyclic code $C_{cyc}(n, k)$ is capable of detecting any error burst of length $n - k$ or less, including the end-round bursts.
- **Theorem**: The fraction of undetectable bursts of length $n - k + 1$ is $1/2^{n-k-1}$.
- **Theorem**: The fraction of undetectable bursts of length $l > n - k + 1$ is $1/2^{n-k}$.
- The cyclic codes are very effective for burst-error detection.
- For example The $C_{cyc}(7, 4)$ generated by $g(X) = 1 + X + X^3$ has minimum distance of 3.
  - It is capable of detecting any combination of two or fewer random errors
  - It is also capable detecting any burst of length 3 or less
  - It also detects many bursts of length greater than 3.

Cyclic redundancy check code for Ethernet standard

- One of the interesting applications of cyclic codes is the cyclic redundancy check (CRC) code untilized in Ethernet protocol.
- Redundancy calculated by a cyclic code is placed in the frame check sequence (FCS) field.
- This cyclic code uses a generator polynomial of degree 32. It means it can generate 32 redundancy bits.
- The information bits in the data packet are considered as mesage vector $m(X)$.
- The reduancy bits are resulted from the remainder of the division of the shifted message polynomial $X^{n-k}m(X)$ by g(X).
- The reciever does the same operation on the message bits.
  - If the redundancy calcualted at the receiver is equal to the redundancy sent in the FCS, the packet is accepted as a valid one.
  - Otherwise, a retransmission of the packet is required.

Cyclic redundancy check code for Ethernet standard

Table: Minimum Hamming distance for different packet configuration in the standard Ethernet protocol

Code length n	Minimum Hamming distance d_{min}
3007-12,144	4
301-3006	5
204-300	6
124-203	7
90-123	8

- Minimum Hamming distance is a function of the code length.
- The error-detection capability is variable with the code length.
- Depending on the packet length, 3 to 7 random errors are always detectable, as well as certain patterns of much larger number of random errors and many bursts error patterns.