ECS455: Chapter 4

Multiple Access

4.5 Cyclic Codes ← a kind of linear block codes.

Note that this topic is not directly related to DSSS nor multiple access. It is a kind of error control codes. However, the technique used are quite similar to the generation of m-sequence and hence we would like to discuss it here.

Dr.Prapun Suksompong
prapun.com/ecs455

Office Hours:
BKD, 6th floor of Sirindhralai building

Tuesday	14:20-15:20
Wednesday	14:20-15:20
Friday	9:15-10:15

MATLAB: circshift

- $\underline{r}'$=`circshift(`$\underline{r}$`,[0,`Δ`])`
  $\underline{r}'$=`circshift(`$\underline{r}$`,`Δ`,2)`
  circularly shifts the elements in a **row vector** $\underline{r}$ to the right by Δ positions.
  - `circshift([1 2 3 4 5],[0 3])=[3 4 5 1 2]`
- $\vec{v}'$=`circshift(`$\vec{v}$`,`Δ`)`
  $\vec{v}'$=`circshift(`$\vec{v}$`,[`Δ`,0])`
  $\vec{v}'$=`circshift(`$\vec{v}$`,`Δ`,1)`
  circularly shifts the elements in a **column vector** $\vec{v}$ down by Δ positions.

MATLAB: demo

```
>> r = 1:5
r =
     1     2     3     4     5
```

```
>> circshift(r,[0,3])
ans =
     3     4     5     1     2

>> circshift(r,3,2)
ans =
     3     4     5     1     2
```

```
>> circshift(r,3)
Warning: CIRCSHIFT(X,K) with scalar K and where size(X,1)==1
will change behavior in future versions. To retain current
behavior, use CIRCSHIFT(X,[K,0]) instead.
ans =
     1     2     3     4     5
```


MATLAB: demo

```
>> v = (1:5)'
v =
     1
     2
     3
     4
     5
```

```
>> circshift(v,[3,0])
ans =
     3
     4
     5
     1
     2
```

```
>> circshift(v,3,1)
ans =
     3
     4
     5
     1
     2
```

```
>> circshift(v,3)
ans =
     3
     4
     5
     1
     2
```

Linear Cyclic Codes

- Definition: A linear code is **cyclic** if a cyclic shift of any valid codeword is still a valid codeword.
  - Lead to more practical implementation.
  - Allow their encoding and decoding functions to be of much lower complexity than the matrix multiplications
- Block codes used in FEC systems are almost always cyclic codes [C&C, 2009, p. 611][G, 2005, p. 220].
- CRC = cyclic redundancy check
  - Invented by W. Wesley Peterson in 1961

Ex. Codebook of a Systematic Cyclic Code

message

k = # bits in $\underline{m}$ = 4

n = # bits in $\underline{c}$ = 7

codeword

0000000
0000000

1010001
1101000
0110100

$\underline{\mathbf{m}}$	$\underline{\mathbf{c}}$
0000	0000000
0001	1010001
0010	1110010
0011	0100011
0100	0110100
0101	1100101
0110	1000110
0111	0010111
1000	1101000
1001	0111001
1010	0011010
1011	1001011
1100	1011100
1101	0001101
1110	0101110
1111	1111111

Associating Vectors with Polynomials

Note that the index starts with 0.

$$\underline{\mathbf{c}} = (c_0, c_1, c_2, \ldots, c_i, \ldots, c_{n-2}, c_{n-1})$$

$$\Updownarrow$$

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_i x^i + \cdots + c_{n-1} x^{n-1}$$

arbitrary variable

The powers of x denote the positions of the bits represented by the corresponding coefficients.

Each codeword has n bits. So, the degree of $c(x)$ is $n-1$.

Example

$$\underline{\mathbf{c}} = 1010011 \Longleftrightarrow c(x) = 1 + 0x + 1x^2 + 0x^3 + 0x^4 + 1x^5 + 1x^6$$

Similarly,

Each message block has k bits. So, the degree of $m(x)$ is $k-1$.

$$\underline{\mathbf{m}} = (m_0, m_1, \ldots, m_{k-1}) \Longleftrightarrow m(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_{k-1} x^{k-1}$$

Message polynomial

Long Division (for numbers)

quotient 13
divisor $6\overline{)83}$ dividend
6
23
18
5 remainder

Many way to write equations that describe the results:

- $83 = 6 \times 13 + 5$
- $\frac{83}{6} = 13 + \frac{5}{6}$
- $83 \equiv 5 \pmod 6$

13
$6\overline{)78}$
6
18
18
0

- Dividing 78 by 6 leaves no remainder
- $78 \equiv 0 \bmod 6$
- 78 is a multiple of 6
- 6 divides 78
- 6 is a divisor of 78
- 78 is divisible by 6
- 6 is a factor of 78
- $6 \mid 78$

Polynomial (Long) Division

$q(x)$

quotient

$$
\begin{array}{rl}
 & \boxed{x^2+1x+3} \\
\text{divisor } x-3 & \overline{)\,x^3-2x^2+0x-4} \text{ dividend} \\
 & \underline{x^3-3x^2} \\
 & +x^2+0x \\
 & \underline{+x^2-3x} \\
 & +3x-4 \\
 & \underline{+3x-9} \\
\text{remainder} & +5
\end{array}
$$

$r(x)$

Many way to write equations that describe the results:

$$x^3-2x^2-4=(x-3)\underbrace{(x^2+x+3)}_{q(x)}+\underbrace{5}_{r(x)}$$

$$\frac{x^3-2x^2-4}{x-3}=x^2+x+3+\frac{5}{x-3}$$

$$x^3-2x^2-4\equiv 5 \pmod{(x-3)}$$

[https://en.wikipedia.org/wiki/Polynomial_long_division]

mod 2 addition and multiplication

Polynomial (Long) Division in GF(2)

Have only 0, 1 (no 2, 3, 4, ... no negative numbers)

$$
\begin{array}{rl}
 & x^3 + \qquad\qquad 1 \quad \xleftarrow{} q(x) \\
x^3+x^2+1 & \overline{)\,x^6+x^5+\qquad\quad x^2+\ 1} \quad c_1(x) \\
 & \underline{x^6+x^5+\quad x^3} \\
 & \qquad\quad x^3+x^2+\ 1 \\
 & \qquad\quad \underline{x^3+x^2+\ 1} \\
 & \qquad\qquad\qquad 0 \quad \text{No remainder}
\end{array}
$$

$- \longrightarrow +$

$(-x = x$ in $GF(2))$

$1 \oplus 1 = 0$

$g(x)$

$r(x)$

$$x^6+x^5+x^2+1\equiv 0 \pmod{(x^3+x^2+1)}$$

$$
\begin{array}{rl}
 & x^3 \quad \xleftarrow{} q(x) \\
x^3+x^2+1 & \overline{)\,x^6+x^5+\quad x^3+x^2+\ 1} \quad c_2(x) \\
 & \underline{x^6+x^5+\quad x^3} \\
 & \qquad\qquad x^2+\ 1 \quad r(x)
\end{array}
$$

The degree here is already < 3. So, we stop the long division.

$$x^6+x^5+x^3+x^2+1\equiv (x^2+1) \pmod{(x^3+x^2+1)}$$

Generator Polynomial

- Cyclic codes are generated via a **generator polynomial** instead of a generator matrix.
- $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$
- Degree $= n - k$
- $g_0 = g_{n-k} = 1$
- Is a divisor of $x^n - 1$.

This makes the code satisfy the circular shift property.

- $c(x)$ is a valid codeword iff $g(x)$ divides $c(x)$ with no remainder.

Two popular ways to generate cyclic code:

1. Non-systematic: $c(x) = m(x)g(x)$
2. Systematic: $c(x) = x^{n-k}m(x) + r(x)$

They give different codes.
If systematic coding is required, then 2 is the method of choice.

Example

- Consider a cyclic code with generator polynomial
$$g(x) = 1 + x^2 + x^3.$$
- Determine if the codeword described by each of the following polynomials is a valid codeword for this generator polynomial.

1010011 • $c_1(x) = 1 + x^2 + x^5 + x^6$

$g(x)$ divides $c_1(x)$ with no remainder $\Rightarrow$ $c_1(x)$ corresponds to a codeword.

1011011 • $c_2(x) = 1 + x^2 + x^3 + x^5 + x^6$

Look at $\frac{c_2(x)}{g(x)}$. There is a remainder of x^2+1 in this division. Therefore, $c_2(x)$ does not correspond to a valid codeword.

Generation of Systematic Cyclic Code

$$c(x) = x^{n-k}m(x) + r(x)$$

- Three steps:

1. Multiply the message polynomial $m(x)$ by x^{n-k}
2. Divide $x^{n-k}m(x)$ by $g(x)$ to get the remainder polynomial $r(x)$.
   - $r(x) \equiv x^{n-k}m(x) \pmod{g(x)}$
3. Substract (add) $r(x)$ from (to) $x^{n-k}m(x)$

- The polynomial multiplications are straightforward to implement, and the polynomial division is easily implemented with a feedback shift register.
- Thus, codeword generation for systematic cyclic codes has very low cost and low complexity.

Generation of Systematic Cyclic Code

$$c(x) = x^{n-k}m(x) - r(x)$$

- $x^{n-k}m(x)$
  - Shift the message bits to the k rightmost digits of the codewords
  - The first $n-k$ bits are "blank"
    - These $n-k$ bits are to be "filled" by $r(x)$.
- By construction,
  - $\deg\big(r(x)\big) < \deg\big(g(x)\big) = n-k$
    - $\deg\big(r(x)\big) \le n-k-1$
    - Correspond to $n-k$ bits.
  - $\dfrac{x^{n-k}m(x)}{g(x)} = q(x) + \dfrac{r(x)}{g(x)}$
    - $x^{n-k}m(x) - r(x) = q(x)g(x)$

Example

- Consider a systematic cyclic (7,4) code whose generator polynomial is $g(x) = 1 + x + x^3$.
- Suppose the message is 0011. Find the corresponding codeword.

$\underline{m} = 0011 \iff m(x) = 0 + 0x + 1x^2 + 1x^3 = x^2 + x^3$

$x^{n-k} m(x) = x^3 m(x) = x^5 + x^6$

$= 0 + 0x + 0x^2 + 0x^3 + 0x^4 + 1x^5 + 1x^6$

can be shifted

$c(x) = x^{n-k} m(x) + r(x)$

$= 0 + 1x + 0x^2 + 0x^3 + 0x^4 + 1x^5 + 1x^6$

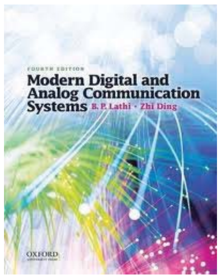
So, $\underline{c} = 0100011$

$$
\begin{array}{r}
x^3 + x^2 + x \\
x^3 + x + 1 \overline{\smash{)}\, x^6 + x^5} \\
x^6 + x^4 + x^3 \\
\hline
x^5 + x^4 + x^3 \\
x^5 + x^3 + x^2 \\
\hline
x^4 + x^2 \\
x^4 + x^2 + x \\
\hline
x
\end{array}
$$

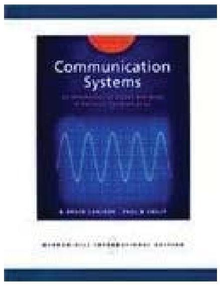
$010 \iff r(x)$

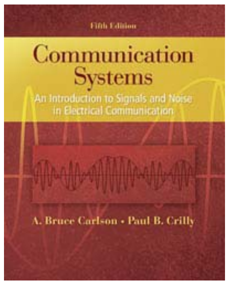
88

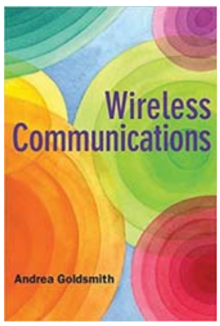
References: Cyclic Codes



- Lathi and Ding, ***Modern Digital and Analog Communication Systems***, 2009
  - [TK5101 L333 2009]
  - Section 15.4 p. 918-923
- Carlson and Crilly, ***Communication Systems: An Introduction to Signals and Noise in Electrical Communication***, 2010
  - [TK5102.5 C3 2010]
  - Section 13.2 p. 611-616
- Goldsmith, ***Wireless Communications***, 2005
  - Section 8.2.4 p. 220-222







89