Good afternoon, gentleman!

Today I give you a lecture about cyclic codes.

This lecture consists of three parts:
I Origin and definition of cyclic codes;
? how to find cyclic codes: The Generator Polynomial;
? one Application of the cyclic codes.

I Origin and definition of cyclic codes

We start with a device called a linear shift register. This is commonly used to encode cyclic codes. The codewords are generated by shifting and adding.

I give an example of a shift register with four storage elements and two binary adders.

**Figure 1.1**

![Shift Register Diagram](image)

At the time zero, four binary elements are placed in $a_0, a_1, a_2,$ and $a_3$. After one time interval, $a_0$ is output, $a_1$ is shifted into $a_0$, $a_2$ into $a_1$, $a_3$ into $a_2$, and the new element is the sum $a_0 + a_2 + a_3$. We suppose that the digits 1101 are placed in $a_0$, $a_1$, $a_2$, and $a_3$, and follow the outputs and inputs for seven time intervals.

If the process is continued, the vector (1,1,0,1,0,0,0) will be repeated. This shift register will repeat any vector of length 7 that it has generated from four initial entries in $a_0, a_1, a_2$, and $a_3$. We can regard the initial four positions as information...
Cyclic codes

positions and the whole process as encoding these information positions to obtain a length 7 codeword (a linear code). This code has the property that whenever \((a_0, a_1, a_2, a_3, a_4, a_5, a_6)\) is a codeword, so is \((a_6, a_0, a_1, a_2, a_3, a_4, a_5)\) also. That means, whenever a vector is in the code, so are all of its cyclic shifts. We can see this in table 1.2.

**Table 1.2** A Repeated Vector

<table>
<thead>
<tr>
<th>outputs</th>
<th>a₀</th>
<th>a₁</th>
<th>a₂</th>
<th>a₃</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 1 0 1 1</td>
<td>1 1 1 0 0</td>
<td>T₀</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 1 0</td>
<td>1 1 1 0 0</td>
<td>T₁</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 1 0 0</td>
<td>1 1 1 0 0</td>
<td>T₂</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 1 0 0 0</td>
<td>1 1 1 0 0</td>
<td>T₃</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 1 0 0 0 1</td>
<td>1 1 1 0 0</td>
<td>T₄</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 1 0 0 0 1 1</td>
<td>1 1 1 0 0</td>
<td>T₅</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 1 0 0 1 1 0</td>
<td>1 1 1 0 0</td>
<td>T₆</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 1 0 0 1 1 0 1</td>
<td>1 1 1 0 0</td>
<td>T₇</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each vector will be repeated, and the last seven digits, which come out of the shift register after any number of shifts, form a vector of the code.

When discussing cyclic codes, we number \(n\) coordinate positions with 0, 1, 2, \(\ldots\), \(n-1\).

**Definition of cyclic codes**

An \([n, k]\) code \(C\) means, the length of code is \(n\), the number of information symbols is \(k\). or we can say an \([n, k]\) binary code \(C\) is a \(k\)—dimensional Subspace of space \(V\).
Cyclic codes

An \([ n , k ]\) code \( C \) is called cyclic if whenever \( X = ( a_0, a_1, a_2, \ldots, a_{n-1} ) \) is in \( C \), so is its first cyclic shift \( Y = ( a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2} ) \). Notice that this means that \( ( a_{n-2}, a_{n-1} a_0, a_1, a_2, \ldots, a_{n-3} ) \) is the first cyclic shift of \( y \), and all the other cyclic shifts of \( X \) are also in \( C \).

When considering cyclic codes, it is useful to let a vector \( ( a_0, a_1, a_2, \ldots, a_{n-1} ) \) correspond to a polynomial \( a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \). Then \( ( a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2} ) \) correspond to \( a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2} x^{n-1} \).

Note that this polynomial equals to the following polynomial

\[
( a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} ) x \pmod{(x^n - 1)}
\]

from that we can get a mathematical model: \( R_n = F(x) / (x^n - 1) \), which consists of congruence classes of polynomials in \( F(x) \) modulo \( (x^n - 1) \), these are polynomials of degree less than \( n \). Polynomials are added and subtracted in \( R_n \) as in \( F(x) \), but multiplication is modulo \( (x^n - 1) \). Obviously, if we have two polynomials \( a(x) \) and \( b(x) \), their product in \( F(x) \) is

\[
a(x) \cdot b(x) = c(x) \cdot (x^n - 1) + r(x)
\]

with the degree of \( r(x) \) less than the degree of \( (x^n - 1) \) by the division algorithm. We regard \( R_n \) as the product of \( a(x) \) and \( b(x) \) when we consider \( R_n \) to be all polynomials in \( F(x) \) of degree less than \( n \) with multiplication modulo \( (x^n - 1) \). Both \( F(x) \) and \( R_n \) are examples of the algebraic structure defined next.

Definition of commutative ring \( R \)

A **commutative ring** \( R \) with unit is a set with two operations, \(+\) (plus) and \(\cdot\) (times), with the following properties:

1. \( R \) is closed under \(+\) (plus) and \(\cdot\) (times);
2. \( R \) is an abelian group under \(+\) (plus);
3. The associative law for multiplication holds \( a (bc) = (ab)c \) for all a, b, and c in \( R \);
4. Multiplication is commutative, \( ab = ba \) for all a and b in \( R \);
5. \( R \) has identity 1 for multiplication \( a \cdot 1 = 1 \cdot a \) for all a in \( R \);
6. The distributive law holds \( a(b+c) = ab + ac \) for all a, b, and c in \( R \);

Definition of Ideal
Cyclic codes

An Ideal $I$ in a commutative ring $R$ is a set of elements in $R$ satisfying the following two conditions:

(i) If $a$ is in $I$, then $ab$ is in $I$ for $b$ in $R$;
(ii) If $a$ and $b$ are in $I$, then $a+b$ and $a-b$ are also in $I$;

Theorem 1

A set of elements $S$ in $R^n$ corresponds to a cyclic code $C$ if $S$ is an Ideal in $R^n$.

(note: proof is omitted, if you are interested in that, you can come to me after the lecture.)

Now let us see an example.

Let $V$ be the space of all binary 3-tuples. We simultaneously locate all binary cyclic codes in $V$ and Ideals in $R_3$, and indicate corresponding vectors:

<table>
<thead>
<tr>
<th>Code</th>
<th>$V$</th>
<th>$R_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>(0,0,0)</td>
<td>0</td>
</tr>
<tr>
<td>$C_2$</td>
<td>(0,0,0)</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>(1,1,1)</td>
<td>1+x+x^2</td>
</tr>
<tr>
<td>$C_3$</td>
<td>(0,0,0)</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>(1,1,0)</td>
<td>1+x</td>
</tr>
<tr>
<td></td>
<td>(0,1,1)</td>
<td>x+x^2</td>
</tr>
<tr>
<td></td>
<td>(1,0,1)</td>
<td>1+x^2</td>
</tr>
<tr>
<td>$C_4$</td>
<td>All of V</td>
<td>All of $R_3$</td>
</tr>
</tbody>
</table>

Now we can say, a cyclic code is either a code closed under the cyclic shift or an Ideal in $R_n$.

? how to find cyclic codes: The Generator Polynomial

In order to find cyclic codes, at first we learn some theory, after that we will see an example.

The following theorem tells us explicitly how to find the generator of a cyclic code: we consider $C$ as consisting of representatives of degree less than $n$ of the congruence classes of multiples of $g(x)$ modulo($x^n$-1).
Cyclic codes

The polynomial \( f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n \), if \( a_n = 1 \), the polynomial of degree \( n \) is called monic.

**Theorem 2**

*If \( C \) is an Ideal (i.e. a cyclic code of length \( n \)) in \( R_n = F(x) / (x^n - 1) \), let \( g(x) \) be the monic polynomial of smallest degree in \( C \). Then \( g(x) \) is uniquely determined and \( C = \langle g(x) \rangle \).*

**Theorem 3**

*If \( C \) is an Ideal in \( R_n \), the unique monic polynomial generator, \( g(x) \), of \( C \) of smallest degree divides \( x^n - 1 \), and conversely, if a polynomial \( g(x) \) in \( C \) divides \( x^n - 1 \), then \( g(x) \) has the lowest degree in \( \langle g(x) \rangle \).*

This says that in order to construct a cyclic code, we need to factor \( x^n - 1 \). When considering binary cyclic codes, we assume that \( n \) is odd since in that case \( x^n - 1 \) has distinct factors.

**Definition of The Generator Polynomial**

*The monic polynomial \( g(x) \) of smallest degree in \( C \) is called The Generator Polynomial in \( C \).*

**Theorem 4**

*If the degree of \( g(x) \) is \( n-k \), then the dimension of \( C = \langle g(x) \rangle \) is \( k \). If \( g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_{n-k} x^{n-k} \), then a generator matrix of \( C \) is the following*

\[
\begin{bmatrix}
g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\
0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\
0 & 0 & g_0 & \cdots & g_{n-k-2} & g_{n-k-1} & g_{n-k} & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & g_{n-k}
\end{bmatrix}
\]

*If we can factor \( x^n - 1 \), we can construct all cyclic codes of length \( n \).*
As an example, we construct binary cyclic codes for \( n = 7 \). The first thing to do is to factor \( x^7 - 1 \), which we know how to do. \( x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3) \). This factorization gives us all cyclic codes of \( x^7 - 1 \).

Consider \( C = \langle g(x) \rangle \) where \( g(x) = 1 + x + x^3 \). Then \( C \) is four-dimensional and has the following generator matrix:

\[
\begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1
\end{bmatrix}
\]

We recognize this as our shift register code example at the beginning.

**Application**

Cyclic codes are an important class of codes for many reasons. One is that they can be efficiently encoded by means of shift registers. There are also decoding schemes utilizing shift registers. Many important codes, such as the Hamming codes, can be represented as cyclic codes.

The presentation of Hamming \([7,4,3]\) code as a cyclic code is

\[
\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
2 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
3 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
4 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
5 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
6 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
7 & 0 & 0 & 0 & 1 & 1 & 0 & 1
\end{array}
\]

That is all.

Thank you for your attention!
Cyclic codes

References
