Part III

Cyclic codes

CHAPTER 3: CYCLIC CODES and CHANNEL CODES

Cyclic codes are special linear codes of large interest and importance because

- They posses a rich algebraic structure that can be utilized in a variety of ways.
- They have extremely concise specifications.
- They can be efficiently implemented using simple shift registers.
- Most of the practically very important codes are cyclic.

Channel codes allow to encode streams of data (bits).

IMPORTANT NOTE

In order to specify a binary code with 2^k codewords of length n one may need to write down

$$2^k$$

codewords of length n.

In order to specify a linear binary code of the dimension k with 2^k codewords of length n it is sufficient to write down

$$k$$

codewords of length n.

In order to specify a binary cyclic code with 2^k codewords of length n it is sufficient to write down

$$1$$

codeword of length n.

BASIC DEFINITION AND EXAMPLES

Definition A code C is cyclic if

(i) C is a linear code;

(ii) any cyclic shift of a codeword is also a codeword, i.e. whenever $a_0, \dots a_{n-1} \in C$, then also $a_{n-1}a_0 \dots a_{n-2} \in C$.

Example

(i) Code $C = \{000, 101, 011, 110\}$ is cyclic.

(ii) Hamming code $Ham(3,2)$: with the generator matrix

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

is equivalent to a cyclic code.

(iii) The binary linear code $\{0000, 1001, 0110, 1111\}$ is not cyclic, but it is equivalent to a cyclic code.

(iv) Is Hamming code $Ham(2,3)$ with the generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

(a) cyclic?

(b) equivalent to a cyclic code?

FREQUENCY of CYCLIC CODES

Comparing with linear codes, cyclic codes are quite scarce. For example, there are 11 811 linear [7,3] binary codes, but only two of them are cyclic.

Trivial cyclic codes. For any field F and any integer $n \geq 3$ there are always the following cyclic codes of length n over F:

- No-information code - code consisting of just one all-zero codeword.
- Repetition code - code consisting of codewords (a, a, ...,a) for $a \in F$.
- Single-parity-check code - code consisting of all codewords with parity 0.
- No-parity code - code consisting of all codewords of length n

For some cases, for example for $n = 19$ and $F = GF(2)$, the above four trivial cyclic codes are the only cyclic codes.

EXAMPLE of a CYCLIC CODE

The code with the generator matrix

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

has codewords

$$c_1 = 1011100 \qquad c_2 = 0101110 \qquad c_3 = 0010111$$
$$c_1 + c_2 = 1110010 \qquad c_1 + c_3 = 1001011 \qquad c_2 + c_3 = 0111001$$
$$c_1 + c_2 + c_3 = 1100101$$

and it is cyclic because the right shifts have the following impacts

$$c_1 \rightarrow c_2, \qquad c_2 \rightarrow c_3, \qquad c_3 \rightarrow c_1 + c_3$$
$$c_1 + c_2 \rightarrow c_2 + c_3, \qquad c_1 + c_3 \rightarrow c_1 + c_2 + c_3, \qquad c_2 + c_3 \rightarrow c_1$$
$$c_1 + c_2 + c_3 \rightarrow c_1 + c_2$$

POLYNOMIALS over GF(q)

A codeword of a cyclic code is usually denoted

$$a_0 a_1 \dots a_{n-1}$$

and to each such a codeword the polynomial

$$a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$$

will be associated.

NOTATION: $F_q[x]$ denotes the set of all polynomials over $GF(q)$.

$deg(f(x))$ = the largest m such that x^m has a non-zero coefficient in $f(x)$.

Multiplication of polynomials If $f(x)$, $g(x) \in Fq[x]$, then

$$deg(f(x)g(x)) = deg(f(x)) + deg(g(x)).$$

Division of polynomials For every pair of polynomials $a(x)$, $b(x) \neq 0$ in $F_q[x]$ there exists a unique pair of polynomials $q(x)$, $r(x)$ in $F_q[x]$ such that

$$a(x) = q(x)b(x) + r(x), deg(r(x)) < deg(b(x)).$$

Example Divide $x^3 + x + 1$ by $x^2 + x + 1$ in $F_2[x]$.
Definition Let $f(x)$ be a fixed polynomial in $F_q[x]$. Two polynomials $g(x)$, $h(x)$ are said to be congruent modulo $f(x)$, notation

$$g(x) \equiv h(x) (\text{mod } f(x)),$$

if $g(x) - h(x)$ is divisible by $f(x)$.

RING of POLYNOMIALS

The set of polynomials in $F_q[x]$ of degree less than $deg(f(x))$, with addition and multiplication modulo $f(x)$, forms a **ring denoted** $F_q[x]/f(x)$.

Example Calculate $(x+1)^2$ in $F_2[x]/(x^2+x+1)$. It holds

$$(x+1)^2 = x^2 + 2x + 1 \equiv x^2 + 1 \equiv x (\text{mod } x^2 + x + 1).$$

How many elements has $F_q[x]/f(x)$?
Result $|F_q[x]/f(x)| = q^{deg(f(x))}$.

Example Addition and multiplication in $F_2[x]/(x^2+x+1)$

+	0	1	x	1+x
0	0	1	x	1+x
1	1	0	1+x	x
x	x	1+x	0	1
1+x	1+x	x	1	0

•	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
1+x	0	1+x	1	x

Definition A polynomial $f(x)$ in $F_q[x]$ is said to be reducible if $f(x) = a(x)b(x)$, where $a(x)$, $b(x) \in F_q[x]$ and

$$deg(a(x)) < deg(f(x)), \qquad deg(b(x)) < deg(f(x)).$$

If $f(x)$ is not reducible, then it is said to be irreducible in $F_q[x]$.
Theorem The ring $F_q[x]/f(x)$ is a field if $f(x)$ is irreducible in $F_q[x]$.