Cyclic and convolution codes

Cyclic codes are of interest and importance because

- They posses 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*.
- Many practically important codes are cyclic.

Convolution codes allow to encode streams od 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 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 $a_0, \ldots a_{n-1} \in C$, then also $a_{n-1}\, a_0 \ldots a_{n-2} \in C$.

Example

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

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

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

is equivalent to a cyclic code.

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

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

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

(a) cyclic?

(b) equivalent to a cyclic code?

FREQUENCY of CYCLIC CODES

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

Trivial cyclic codes. For any field F and any integer $n >= 3$ 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 $(a, a, \ldots, a)$ 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

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

has codewords

$c_1 = 1011100$ $c_2 = 0101110$ $c_3 = 0010111$

$c_1 + c_2 = 1110010$ $c_1 + c_3 = 1001011$ $c_2 + c_3 = 0111001$

$c_1 + c_2 + c_3 = 1100101$

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

$c_1 \to c_2,$ $c_2 \to c_3,$ $c_3 \to c_1 + c_3$

$c_1 + c_2 \to c_2 + c_3,$ $c_1 + c_3 \to c_1 + c_2 + c_3,$ $c_2 + c_3 \to c_1$

$c_1 + c_2 + c_3 \to c_1 + c_2$

POLYNOMIALS over GF(q)

A codeword of a cyclic code is usually denoted

$$a_0\, a_1 \ldots a_{n-1}$$

and to each such a codeword the polynomial

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

is associated.

$F_q[x]$ 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) $\in F_q[x]$, 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

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

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** $\mathbf{F_q[x]/f(x)}$.

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

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

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, it is irreducible in $F_q[x]$.

Theorem The ring $F_q[x]$ / f(x) is a <u>field</u> if f(x) is irreducible in $F_q[x]$.

FIELD R_n, $R_n = F_q[x] / (x^n - 1)$

Computation modulo $x^n - 1$

Since $x^n \equiv 1 \pmod{x^n - 1}$ we can compute f(x) mod x^n -1 as follow:
In f(x) replace x^n by 1, x^{n+1} by x, x^{n+2} by x^2, x^{n+3} by x^3, …

Identification of words with polynomials

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

Multiplication by x in R_n corresponds to a single cyclic shift

$$x (a_0 + a_1 x + \ldots a_{n-1} x^{n-1}) = a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2} x^{n-1}$$

Algebraic characterization of cyclic codes

Theorem A code C is cyclic if C satisfies two conditions

(i) $a(x), b(x) \in C \Rightarrow a(x) + b(x) \in C$

(ii) $a(x) \in C, r(x) \in R_n \Rightarrow r(x)a(x) \in C$

Proof

(1) Let C be a cyclic code. C is linear $\Rightarrow$ (i) holds.

(ii) Let $a(x) \in C$, $r(x) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1}$

$$r(x)a(x) = r_0 a(x) + r_1 x a(x) + \ldots + r_{n-1} x^{n-1} a(x)$$

is in C by (i) because summands are cyclic shifts of $a(x)$.

(2) Let (i) and (ii) hold

- Taking $r(x)$ to be a scalar the conditions imply linearity of C.
- Taking $r(x) = x$ the conditions imply cyclicity of C.

CONSTRUCTION of CYCLIC CODES

Notation If $f(x) \in R_n$, then

$$\langle f(x) \rangle = \{r(x)f(x) \mid r(x) \in R_n\}$$

(multiplication is modulo $x^n - 1$).

Theorem For any $f(x) \in R_n$, the set $\langle f(x) \rangle$ is a cyclic code (generated by f).

Proof We check conditions (i) and (ii) of the previous theorem.

(i) If $a(x)f(x) \in \langle f(x) \rangle$ and $b(x)f(x) \in \langle f(x) \rangle$, then

$$a(x)f(x) + b(x)f(x) = (a(x) + b(x))\, f(x) \in \langle f(x) \rangle$$

(ii) If $a(x)f(x) \in \langle f(x) \rangle$, $r(x) \in R_n$, then

$$r(x)\,(a(x)f(x)) = (r(x)a(x))\, f(x) \in \langle f(x) \rangle.$$

Example $C = \langle 1 + x^2 \rangle$, $n = 3$, $q = 2$.
We have to compute $r(x)(1 + x^2)$ for all $r(x) \in R_3$.

$$R_3 = \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\}.$$

Result

$$C = \{0, 1 + x, 1 + x^2, x + x^2\}$$

$$C = \{000, 011, 101, 110\}$$

Characterization theorem for cyclic codes

We show that all cyclic codes C have the form $C = \langle f(x) \rangle$ for some $f(x) \in R_n$.

Theorem Let C be a non-zero cyclic code in R_n. Then

- there exists unique monic polynomial $g(x)$ of the smallest degree such that
- $C = \langle g(x) \rangle$
- $g(x)$ is a factor of $x^n - 1$.

Proof

(i) Suppose $g(x)$ and $h(x)$ are two monic polynomials in C of the smallest degree. Then the polynomial $g(x) - h(x) \in C$ and it has a smaller degree and a multiplication by a scalar makes out of it a monic polynomial. If $g(x) \neq h(x)$ we get a contradiction.

(ii) Suppose $a(x) \in C$.

Then

$$a(x) = q(x)g(x) + r(x) \qquad (\deg r(x) < \deg g(x))$$

and

$$r(x) = a(x) - q(x)g(x) \in C.$$

By minimality

$$r(x) = 0$$

and therefore $a(x) \in \langle g(x) \rangle$.

Characterization theorem for cyclic codes

(iii) Clearly,

$$x^n - 1 = q(x)g(x) + r(x) \quad \text{with} \quad deg\, r(x) < deg\, g(x)$$

and therefore $r(x) \equiv -q(x)g(x) \pmod{x^n - 1}$ and

$$r(x) \in C \Rightarrow r(x) = 0 \Rightarrow g(x) \text{ is a factor of } x^n - 1.$$

GENERATOR POLYNOMIALS

Definition If for a cyclic code C it holds

$$C = \langle g(x) \rangle,$$

then g is called the **generator polynomial** for the code C.

HOW TO DESIGN CYCLIC CODES?

The last claim of the previous theorem gives a recipe to get all cyclic codes of given length n.

Indeed, all we need to do is to find all factors of

$$x^n - 1.$$

Problem: Find all binary cyclic codes of length 3.

Solution: Since

$$x^3 - 1 = \underbrace{(x + 1)(x^2 + x + 1)}_{\text{both factors are irreducible in } GF(2)}$$

we have the following generator polynomials and codes.

Generator polynomials	Code in R_3	Code in $V(3,2)$
1	R_3	$V(3,2)$
$x + 1$	$\{0, 1 + x, x + x^2, 1 + x^2\}$	{000, 110, 011, 101}
$x^2 + x + 1$	$\{0, 1 + x + x^2\}$	{000, 111}
$x^3 - 1$ (= 0)	$\{0\}$	{000}

Design of generator matrices for cyclic codes

Theorem Suppose C is a cyclic code of codewords of length n with the generator polynomial

$$g(x) = g_0 + g_1 x + \dots + g_r x^r.$$

Then $dim(C)$ = n - r and a generator matrix G_1 for C is

$$G_1 = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ .. & .. & & & & & & & & .. \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & g_0 & \dots & g_r \end{pmatrix}$$

Proof

(i) All rows of G_1 are linearly independent.

(ii) The n - r rows of G represent codewords

$$g(x),\ xg(x),\ x^2 g(x), \dots,\ x^{n-r-1} g(x)$$

(*)

(iii) It remains to show that every codeword in C can be expressed as a linear combination of vectors from (*).

Inded, if $a(x) \in C$, then

$$a(x) = q(x)g(x).$$

Since $deg\ a(x) < n$ we have $deg\ q(x) < n - r$.

Hence

$$q(x)g(x) = (q_0 + q_1 x + \dots + q_{n-r-1} x^{n-r-1})g(x)$$
$$= q_0 g(x) + q_1 x g(x) + \dots + q_{n-r-1} x^{n-r-1} g(x).$$

EXAMPLE

The task is to determine all ternary codes of length 4 and generators for them.

Factorization of $x^4 - 1$ over $GF(3)$ has the form

$$x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1) = (x - 1)(x + 1)(x^2 + 1)$$

Therefore there are $2^3 = 8$ divisors of $x^4 - 1$ and each generates a cyclic code.

Generator polynomial	Generator matrix
1	I_4
x	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x + 1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
$x^2 + 1$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x + 1) = x^2 - 1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x^2 + 1) = x^3 - x^2 + x - 1$	[-1 1 -1 1]
$(x + 1)(x^2 + 1)$	[1 1 1 1]
$x^4 - 1 = 0$	[0 0 0 0]