3. CYCLIC CODES

Cyclic codes are of interest and importance because

- They posses rich algebraic structure that can be utilized in a variety of ways.
- They can be efficiently implemented using simple *shift registers*
- Many practically important codes are cyclic

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 generator matrix

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

is equivalent to a cyclic code.
(iii) The binary linear code $\{0000, 1001, 0110, 1111\}$ is not a cyclic, but it is eqivalent to a cyclic code.
(iv) Is Hamming code $Ham(2, 3)$ with generator matrix

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

(a) cyclic?
(b) equivalent to a cyclic code?

Polynomials over $GF(q)$

Codewords of cyclic codes are 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 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

$$g(x) \equiv h(x) (\bmod\ f(x)),$$

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

Ring of polynomials $F_q[x]/f(x)$

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**.

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

$\cdot$	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

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

If $f(x)$ is not reducible, it is **irreducible** in $F_q[x]$.

Theorem The ring $F_q[x]/f(x)$ is a **field** iff $f(x)$ 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, $\ldots$.

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**

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

Algebraic characterization of cyclic codes

Theorem A code C is cyclic iff 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

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

(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 $C = \langle 1 + x^2 \rangle$.
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

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

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

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

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

and

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

By minimality

$$r(x) = 0$$

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

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

and therefore

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

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

$$x^n - 1.$$

Example The task is to find all binary cyclic codes of length 3.

Since

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

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

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

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

$$\begin{bmatrix} g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & \ldots & 0 \\ \vdots & \vdots & & & & & & & & \vdots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & g_0 & \ldots & g_r \end{bmatrix}$$

Proof (i) All rows of G are linearly independent.
(ii) The $n - r$ rows of G represent codewords

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

(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

$$\begin{aligned} q(x)g(x) &= (q_0 + q_1 x + \ldots + q_{n-r-1} x^{n-r-1}) g(x) \\ &= q_0 g(x) + q_1 x g(x) + \ldots + q_{n-r-1} x^{n-r-1} g(x). \end{aligned}$$

EXAMPLE

The task is to determine all ternary codes of length 4 and generators for all of 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
$x-1$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x+1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
x^2+1	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x-1)(x+1) = x^2 - 1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x-1)(x^2+1) = x^3 - x^2 + x - 1$	$\begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}$
$(x+1)(x^2+1)$	$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$
$x^4 - 1 = 0$	$\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$

Check polynomials and parity check matrices for cyclic codes

Let C be a cyclic $[n,k]$-code with the generator polynomial $g(x)$ (of degree $n-k$). By the last theorem $g(x)$ is a factor of x^n-1. Hence

$$x^n - 1 = g(x)h(x)$$

for some $h(x)$ of degree k (where $h(x)$ is called the **check polynomial** of C).

Theorem Let C be a cyclic code in R_n with a generator polynomial $g(x)$ and a check polynomial $h(x)$. Then an $c(x) \in R_n$ is a codeword of C iff $c(x)h(x) \equiv 0$.

Proof Note, that $g(x)h(x) = x^n - 1 \equiv 0$
(i) $c(x) \in C \Rightarrow c(x) = a(x)g(x)$ for some $a(x) \in R_n$

$$\Rightarrow c(x)h(x) = a(x)\underbrace{g(x)h(x)}_{\equiv 0} \equiv 0.$$

(ii) $c(x)h(x) \equiv 0$

$$c(x) = q(x)g(x) + r(x), \deg\ r(x) < n-k = \deg\ g(x)$$
$$c(x)h(x) \equiv 0 \Rightarrow r(x)h(x) \equiv 0 \pmod{x^n - 1}$$

Since $\deg(r(x)h(x)) < n-k+k = n$, we have $r(x)h(x) = 0$ in $F[x]$ and therefore

$$r(x) = 0 \Rightarrow c(x) = q(x)g(x) \in C.$$

POLYNOMIAL REPRESENTATION of DUAL CODES

Since $\dim(\langle h(x)\rangle) = n-k = \dim(C^{\perp})$ we might easily be fooled to think that the check polynomial $h(x)$ of the code C generates the dual code $C^{\perp}$.

Reality is "slightly different":

Theorem Suppose C is a cyclic $[n,k]$-code with the check polynomial

$$h(x) = h_0 + h_1x + \ldots + h_kx^k,$$

then
(i) a parity-check matrix for C is

$$H = \begin{bmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_k & \ldots & h_1 & h_0 & \ldots & 0 \\ \vdots & \vdots & & & & & \\ 0 & 0 & \ldots & 0 & h_k & \ldots & h_0 \end{bmatrix}$$

(ii) $C^{\perp}$ is the cyclic code generated by the polynomial

$$\hat{h}(x) = h_k + h_{k-1}x + \ldots + h_0x^k$$

i.e. the **reciprocal polynomial** of $h(x)$.

Proof A polynomial $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ represents a code from C iff $c(x)h(x) = 0$. For $c(x)h(x)$ to be 0 the coefficients at $x^k, \ldots, x^{n-1}$ must be zero, i.e.

$$\begin{aligned} c_0h_k + c_1h_{k-1} + \ldots + c_kh_0 &= 0 \\ c_1h_k + c_2h_{k-1} + \ldots c_{k+1}h_0 &= 0 \\ \vdots \qquad\qquad & \quad \vdots \\ c_{n-k-1}h_k + c_{n-k}h_{k-1} \ldots c_{n-1}h_0 &= 0 \end{aligned}$$

$$c_0 h_k + c_1 h_{k-1} + \ldots + c_k h_0 = 0$$
$$c_1 h_k + c_2 h_{k-1} + \ldots c_{k+1} h_0 = 0$$
$$\vdots \qquad\qquad\qquad\qquad \vdots$$
$$c_{n-k-1} h_k + c_{n-k} h_{k-1} + \ldots + c_{n-1} h_0 = 0$$

Therefore, any codeword $c_0 c_1 \ldots c_{n-1} \in C$ is orthohonal to the word $h_k h_{k-1} \ldots h_0 00 \ldots 0$ and to its cyclic shifts.

Rows of the matrix H are therefore in $C^\perp$. Moreover, since h_k =1, these row-vectors are linearly independent. Their number is $n - k =$ *dim*$(C^\perp)$. Hence H is a generator matrix for $C^\perp$, i.e. a parity-check matrix for C.

In order to show that $C^\perp$ is a cyclic code generated by the polynomial

$$\bar{h}(x) = h_k + h_{k-1} x + \ldots h_0 x^k$$

it is sufficient to show that $\bar{h}(x)$ is a factor of $x^n - 1$.

Observe that $\bar{h}(x) = x^k h(x^{-1})$ and since

$$h(x^{-1}) g(x^{-1}) = (x^{-1})^n - 1$$

we have that

$$x^k h(x^{-1}) x^{n-k} g(x^{-1}) = x^n (x^{-n} - 1) = 1 - x^n$$

and therefore $\bar{h}(x)$ is indeed a factor of $x^n - 1$.

Hamming codes as cyclic codes

Definition (Again!) Let r be a positive integer and let H be an $r \times (2^r - 1)$ matrix whose columns are distinct non-zero vectors of $V(r, 2)$. Then the code having H as its parity-check matrix is called binary **Hamming code** denoted by $Ham(r, 2)$.

It can be shown that binary Hamming codes are equivalent to cyclic codes.

Theorem The binary Hamming code $Ham(r, 2)$ is equivalent to a cyclic code.

Definition If $p(x)$ is an irreducible polynomial of degree r such that x is a primitive element of the field $F[x]/p(x)$, then $p(x)$ is called a primitive polynomial.

Theorem If $p(x)$ is a primitive polynomial over $GF(2)$ degree r, then the cyclic code $\langle p(x) \rangle$ is the code $Ham(r, 2)$.

Example Polynomial $x^3 + x + 1$ is irreducible over $GF(2)$ and x is primitive element of the field $F_2[x]/(x^3 + x + 1)$.

$$F_2[x]/(x^3 + x + 1) =$$
$$\{0, x, x^2, x^3 = x + 1, x^4 = x^2 + x, x^5 = x^2 + x + 1, x^6 = x^2 + 1\}$$

The parity-check matrix for a cyclic version of $Ham(3, 2)$

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

PROOF of THEOREM

The binary Hamming code *Ham*$(r, 2)$ is equivalent to a cyclic code.

It is known from algebra that if $p(x)$ is an irreducible plynomial of degree r, then the ring $F_2[x]/p(x)$ is a field of order 2^r.

In addition, every finite field has a primitive element. Therefore, there exists an element α of $F_2[x]/p(x)$ such that

$$F_2[x]/p(x) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2r-2}\}.$$

Let us identify an element $a_0 + a_1 + \ldots a_{r-1}x^{r-1}$ of $F_2[x]/p(x)$ with the column vector

$$(a_0, a_1, \ldots, a_{r-1})^T$$

and consider the binary $r \times (2^r - 1)$ matrix

$$H = [1 \ \alpha \ \alpha^2 \ \ \ldots \alpha^{2^r-2}].$$

Let now C be the binary linear code having H as a parity check matrix.

Since the columns of H are all distinct non-zero vectors of $V(r, 2)$, $C =$ *Ham*$(r, 2)$.

Putting $n = 2^r - 1$ we get

$$\begin{aligned} C &= \{f_0 f_1 \ldots f_{n-1} \in V(n, 2) \mid f_0 + f_1\alpha + \ldots + f_{n-1}\alpha^{n-1} = 0 \quad (2) \\ &= \{f(x) \in R_n \mid f(\alpha) = 0 \text{ in } F_2[x]/p(x)\} \quad (3) \end{aligned}$$

If $f(x) \in C$ and $r(x) \in R_n$, then $r(x)f(x) \in C$ because

$$r(\alpha)f(\alpha) = r(\alpha) \cdot 0 = 0$$

and therefore, by one of the previous theorems, this version of *Ham*$(r, 2)$ is cyclic.

BCH codes and Reed-Solomon codes

To the most important cyclic codes for applications belong BCH codes and Reed-Solomon codes.

Definition A polynomial p is said to be *minimal* for a complex number x in Z_q if $p(x) = 0$ and p is irreducible over Z_q.

Definition A cyclic code of codewords of length n over Z_q, $q = p^r$, p is a prime, is called **BCH code**[1] of distance d if its generator $g(x)$ is the least common multiple of the minimal polynomials for

$$\omega^l, \omega^{l+1}, \ldots, \omega^{l+d-2}$$

for some l, where

$$\omega \text{ is the primitive } n\text{-th root of unity.}$$

If $n = q^m - 1$ for some m, then the BCH code is called **primitive**.

Definition A **Reed-Solomon** code is a primitive BCH code with $n = q - 1$.

Properties:

- Reed-Solomon codes are self-dual.

[1] BHC stands for Bose and Ray-Chaudhuri and Hocquenghem who discovered these codes.