Information and Coding theory

Lec-21

all of you have opted for 'online exam'

— $\boxed{\text{Mon } 11^{th} \text{ Apr } 2022}$, $\boxed{\text{8-10 AM}}$,

$\boxed{\text{Viva Exam}}$ — @ Mon 4th April, 2022

(n, K) linear blockcode.

— $\boxed{d_{min}}$ can easily be found.

C... Code. $x \equiv (x_1, x_2 . \; x_n)$

Cyclic

any codeword is written as

$$c = (c_{n-1}\ c_{n-2} \dots c_1\ c_0)$$

highest order

least order

$\{0,1\}^n$

A cyclic-shift Leftwards / rightwards on a codeword gives a codeword.

cyclic-shift leftward one-bit gives

$$c' = (c_{n-2} \dots c_1\ c_0\ c_{n-1})$$

Cyclic-shift rightward 4-bits.

$$c'' = (c_3\, c_2\, c_1\, c_0\, c_{n-1} \cdots c_4)$$

Cyclic code: It is a linear code which is invariant under a cyclic-shift.

Exp. $\boxed{(7,4)}$ – Hamming Code

Remark: not all linear codes are cyclic.

Polynomial representation of a n-bit word.

$$\cdots\ a_1\ a_0)$$

$a \equiv (a_{n-1} \; a_{n-2}$

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

Obs. max. degree of any n-bit codewords is $n-1$

Exp. 5-bit code word
$(0\ 1\ 1\ 0\ 1)$

$p(x) = 0x^4 + 1x^3 + 1x^2 + 0x + 1$
$= x^3 + x^2 + 1$

Polynomial algebra.

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

$p_b(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_0$

$\longrightarrow \; p_b(x)$

Then $p_a(x) + p_b(x) = (a_{n-1} + b_{n-1}) x^{n-1} + \dots + (a_0 + b_0)$

For expl. $p_1(x) = x^5 + x^4 + \cancel{x}$

$p_2(x) = x^3 + \cancel{x} + 1$

$p_1(x) + p_2(x) = x^5 + x^4 + x^3 + 1$

<u>Division</u> $\quad p_1(x), \quad p_2(x).$

dividend $\quad$ divisor

$p_1(x) = x^5 + x^4 + x$

$p_2(x) = x^3 + x + 1$

$$x^2 + x + 1 \leftarrow q(x)$$

$$x^3 + x + 1 \;\big)\; x^5 + x^4 + x$$

$$\begin{array}{r}
x^5 + x^3 + x^2 \\
+ \quad \overline{\qquad\qquad\qquad\qquad} \\
x^4 + x^3 + \cancel{x^2} + \cancel{x} \\
x^4 + \cancel{x^2} + \cancel{x} \\
+ \quad \overline{\qquad\qquad\qquad\qquad} \\
\cancel{x^3} \\
\cancel{x^3} + x + 1 \\
+ \quad \overline{\qquad\qquad\qquad\qquad} \\
x + 1 \leftarrow r(x)
\end{array}$$

Given two integers a, b, we always get q, r s.t.

$$\boxed{a = qb + r}$$

q → quotient

r → remainder.

$$\boxed{0 \le r < |b|}$$

↳ Euclidean division algorithm.

$$p_1(x) = q(x)\,p_2(x) + \boxed{r(x)}$$

Notation.

$$\boxed{r(x) = R_{p_2(x)}[p_1(x)]}$$

↳ where $r(x)$ is the remainder when $p_1(x)$ is divided by $p_2(x)$.

If $\quad p_1(x) = p_2(x)\,f(x)$

then $\quad R_{p_2(x)}[p_2(x)\,f(x)] = 0$

n-bit codeword.

Suppose we have an
Then we have a polynomial wrt this
codeword.

$$p \quad \boxed{a \equiv (a_{n-1}\ a_{n-2}\ \ldots\ a_1\ a_0)}$$

$$\longrightarrow \quad p_a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0.$$

Suppose we give a cyclic-shift left ~~word~~
by 1 bit.

$$\longrightarrow \quad a' \equiv (\underline{a_{n-2}}\ a_{n-3}\ \ldots\ a_0\ a_{n-1})$$

$$\longrightarrow \quad p_{a'}(x) = a_{n-2}x^{n-1} + a_{n-3}x^{n-2} + \cdots + a_0 x + a_{n-1}$$

H.W.

We can show that ✓

$$p_{a'}(x) = R_{\underline{x^n+1}}\left[\underbrace{x\, p_a(x)}\right]$$

Exp.

$a = (1,0,1,1,0,0)$ $\boxed{n=6 \;\; 2017}$

$a' = (0\,1\,1\,0\,0\,1)$

$p_a(x) = x^5 + x^3 + x^2$

$x\,p_a(x) = x^6 + x^4 + x^3$

$p_{a'}(x) = x^4 + x^3 + 1 \leftarrow$

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^6 + 1 & x^6 + x^4 + x^3 \\
 & x^6 + 1 \\
\hline
 & x^4 + x^3 + 1
\end{array}
$$

$\leftarrow$ Remainder.

H. W. what about the rightward cyclic shift ?

cyclic ...

Multiplication.

$p_1(x) \longrightarrow$ codewords poly. of deg. $n-1$

$p_2(x) \longrightarrow$ codeword poly of deg $n-1$

$$\deg(p_1(x)p_2(x)) = \deg(p_1) + \deg(p_2)$$

Define $p_1(x) * p_2(x) = p(x)$.

$$\boxed{p(x)} = R_{x^n+1}[\underbrace{p_1(x)\,p_2(x)}_{\text{Standard multiplication}}]$$

Then deg of $p(x) \leq n-1$.

Then

(n, k) - cyclic cod.

Prob. $(i_1\ i_2 \cdots i_k) \longrightarrow (\underbrace{c_1\ c_2 \cdots c_n}_{t})$

Generator polynomials.

$(7, 4)$ Hamming code.

Codeword	codeword poly
$c_0 = (0000000)$	$c_0(x) = 0$
$c_1 = (0001011)$	$c_1(x) = x^3 + x + 1$
$c_2 = (0010110)$	$c_2(x) = x^4 + x^2 + x$
$c_3 = (0011101)$	$c_3(x) = x^4 + x^3 + x^2 + 1$
$c_4 = (0100111)$	$c_4(x) = x^5 + x^2 + x + 1$
$c_5 = (0101100)$	$c_5(x) = x^5 + x^3 + x^2$

$x^3 + x + 1$

Consider $C_1(x) =$

$C_2(x) = x\, C_1(x)$

$C_3(x) = (x+1)\underline{(x^3+x+1)}$

$C_5(x) = x^2\, C_1(x)$

$C_4(x) = (x^2+1)(x^3+x+1)$

H.W.

$$\begin{array}{r|l} & x^2 + 1 \\ \hline x^3 + x + 1 & x^5 + \cancel{x^2} + x + 1 \\ + & x^5 + x^3 + \cancel{x^2} \\ \hline & x^3 + x + 1 \end{array}$$

Q. What is the max degree of $f_i(x)$ s.t. $C_i(x) = \boxed{f_i(x)}\,(x^3+x+1)$

If we consider all polynomials of degree less or equal to $\boxed{3}$ then we can obtain the complete list of codeword polynomial.

Conclusion: $x^{\boxed{3}} + x + 1$ is the generator polynomial of the (7, 4) Hamming code which is (7, 4) binary cyclic code.

H.W.

Facts.

① In any (n, k) cyclic code there exists a unique generator poly.

② If $g(x)$ is the generator poly. for an (n, k) cyclic code then

$$g(x) = g_{n-k} x^{\boxed{n-k}} + g_{n-k-1} x^{n-k-1} + \dots + g_2 x^2 + g_1 x + g_0$$

$g_i \in \{0,1\}$.

$g_{n-k} = 1$, $g_0 = 1$

(3) If we multiply $g(x)$ with every polynomial of degree $k-1$ or less, it generates all the codeword polynomials of an (n,k) cyclic code.

(4) The generator polynomial is ~~the~~ the smallest degree codeword polynomial.

Encoding cyclic code.

2^k

$\bar{i} = (i_{k-1}\ i_{k-2}\ \ldots\ i_1\ i_0)$

Prob. Find $\bar{c} = (c_{n-1}\ c_{n-2}\ \ldots\ c_1\ c_0)$?

Nonsystematic encoding.

$i(x) = i_{k-1} x^{k-1} + i_{k-2} x^{k-2} + \cdots + i_2 x^2 + i_1 x + i_0.$

$$\boxed{c(x) = i(x)\, g(x)}$$

Systematic encoding.

$i(x)$

(n, k), $g(x)$, $i(x)$

Algo.

1. Multiply $i(x)$ by x^{n-k}

   i.e. $i(x)\, x^{n-k}$

2. Divide $\underline{i(x)\, x^{n-k}}$ by $\underline{g(x)}$

$$\longrightarrow \quad r(x) = R_{g(x)}\left[i(x)\, x^{n-k} \right]$$

3. Add $r(x)$ with $i(x)\, x^{n-k}$.

$$\longrightarrow \quad \boxed{c(x) = i(x)\, x^{n-k} + r(x)}$$

Decoding of cyclic codes.

Obs. $g(x)$ is a factor of any codeword polynomial

Suppose $v(x)$ is received word.

The decoder finds

$$r(x) = R_{g(x)}[v(x)]$$

$r(x) = 0$ ~~then~~ if ~~it is~~ $v(x)$ is a codeword.

$\Rightarrow$ if $r(x) \neq 0$ then $v(x)$ is not a codeword polynomial.

Syndrome polynomial:

$$s(x) = R_{g(x)}[v(x)].$$

if $v(x) = c(x)$ then

$s(x) = 0$

error polynomial

Now $\underline{v(x) = c(x) + e(x)}$

$\underline{s(x)} = R_{g(x)}[v(x)]$

$= R_{g(x)}[\underbrace{c(x) + e(x)}]$

H.W. $= \underbrace{R_{g(x)}[c(x)]}_{0} + R_{g(x)}[e(x)]$

$= \boxed{R_{g(x)}[e(x)]}$

$\overset{?}{=} e(x)$

$p(x) \overline{) \; f_1(x) + f_2(x) \;(}$

$\vdots$

$r(x)$

$\hookrightarrow \; r_1(x) = R_{p(x)}[f_1(x)]$

$r_2(x) = R_{p(x)}[f_2(x)]$

$$g(x) = x^3 + x^2 + 1$$

$$e(x) = 1$$

Syndrome terms,

Syndrome	$e(x)$
(0000000)	0
(0000001)	x
(0000010)	x^2
	x^3
	$\vdots$
	x^6

$$g(x) = x^3 + x^2 + 1$$

$$e(x) = x.$$

$$q(x) = 0$$

$$\boxed{e(x) = q(x)\, g(x) + r(x)}$$

Lec-22

Cyclic code — linear code $\{0,1\}^n$

(n, k) — linear code which is closed under cyclic-shifts

$$\boxed{(c_{n-1}\, c_{n-2}\, \ldots\, c_0)}$$

$(7,4)$ Hamming code is a cyclic code.

$i \longrightarrow i(x)$ information

$\bar{c}(x) = \bar{i}(x)\, g(x)$ ← generator poly.

$\underbrace{\sim\sim}_{n-1\ \deg?}$ $\underbrace{\sim\sim}_{k-1}$ $\underbrace{\sim\sim}_{n-k}$

$(i_{k-1}\ i_{k-2} \cdots i_0)$

$r(x) = R_{p(x)}[f(x)]$

$v(x) \leftarrow$ received poly.

$g(x) / v(x)$

$\Rightarrow \quad R_{g(x)}[v(x)] = 0$

$s(x) = R_{g(x)}[e(x)]$, $\begin{cases} c(x) = v(x) + e(x) \\ v(x) = c(x) + e(x) \end{cases}$

Can any poly of deg $(n-k)$ ... code?

Q. generate a cyclic code?

Exp. (7,4) Hamming code

$g(x) = x^3 + x + 1.$

$g(x) \,/\, x^7 + 1,$

$$
\begin{array}{r}
x^4 + x^2 + x + 1 \\
x^3 + x + 1 \overline{\big) \, x^7 + 1} \\
x^7 + x^5 + x^4 \\
\hline
x^5 + x^4 + 1 \\
x^5 + x^3 + x^2 \\
\hline
x^4 + x^3 + \cancel{x^2} + 1 \\
\cancel{x^4} + \cancel{x^2} + x \\
\hline
x^3 + x + 1 \\
x^3 + x + 1 \\
\hline
\end{array}
$$

A poly. $g(x)$ of deg r generates an (n, k) cyclic code, where $k = n-r$ if $g(x)$ divides x^n+1.

$$g(x)\, h(x) = x^n + 1$$

Exp

$$(x^3+x+1)\underbrace{(x^4+x^2+x+1)}_{h(x)} = x^7+1$$

$\Rightarrow$ $h(x) = x^4+x^2+x+1$ is a generator poly for a $(7, 3)$ cyclic code.

$x+1 \mid x^7+1$

Quotient poly $R_{x+1}[x^7+1] = (x^6+x^5+x^4+x^3+x^2+x+1)$

$\Rightarrow$ $x+1$ is a generator poly. for $(7,6)$ code.

generator poly for $(7,1)$.

$(x+1)(x^3+x+1)(x^3+x^2+1) = x^7+1$

irreducible ... x^7+1

Are irre... factor of ...

Cyclic code

$f_1(x) = x+1$ $\longrightarrow$ $(7,6)$

$f_2(x) = x^3 + x^2 + 1$ $\longrightarrow$ $(7,4)$

equivalent

$f_3(x) = x^3 + x + 1$ $\longrightarrow$ $(7,4)$

$f_1(x) f_2(x) = x^4 + \cancel{x^3} + x^2 \ldots$
$+ \cancel{x^3} + x^2 + 1$ $\longrightarrow$ $(7,3)$

$= x^4 + x^2 + x + 1$

equivalent.

$f_2(x) f_3(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ $\longrightarrow$ $(7,1)$

$f_1(x) f_3(x) = x^4 + x^2 + \cancel{x} + x^3 + \cancel{x} + 1$ $\longrightarrow$ $(7,3)$
$= x^4 + x^3 + x^2 + 1$

~~then $g(x)$ is~~

If $g(x) \,/\, x^n + 1$ and $\deg(g(x)) = r$ then $g(x)$ is a generator poly of a (n, k) cyclic code. $r = n - k$.

$$\Rightarrow \quad g(x)\, h(x) = x^n + 1$$

$$h(x) = \frac{\overset{\text{deg } n}{x^n + 1}}{\underset{\text{deg. } n-k}{g(x)}}$$

$\Rightarrow$

Q. $\deg(h(x)) = k$.

$$h(x) = h_k x^k + h_{k-1} x^{k-1} + \dots + h_2 x^2 + h_1 x + h_0.$$

$\boxed{h_k = 1}$, $\boxed{h_0 = 1}$. H.W.

Exp. $h(x) = x^4 + x^2 + x + 1$

the parity-check polynomial.

$\bar{c} = \bar{i}G$

$GH^T = 0$

$\bar{c}H^T = 0$

$s = vH^T$

$\bar{c}(x) = \bar{i}(x)\, g(x)$

$R_{x^n+1}[g(x)\, h(x)] = 0$

$\boxed{R_{x^n+1}[c(x)\, h(x)] = 0}$

$\boxed{s(x) = R_{x^n+1}[v(x)\, h(x)]}$

H.W.

$\bar{i}(x)\, g(x)$

$$\bar{c}(x) = i(x)\, g(x)$$

$$\Rightarrow h(x)\, c(x) = i(x)\, \underbrace{g(x)\, h(x)}_{x^n+1}$$

$$\Rightarrow h(x)\, c(x) = i(x)\,(x^n+1)$$

Dual cyclic code.

Use ~~the~~ parity-check poly $h(x)$ of a cyclic code C to generate another code which is called the dual code ; denoted by C^*.

$\deg(h(x)) = r$

define reciprocal polynomial $h^*(x)$ of $h(x)$ as

$$h^*(x) \doteq x^r h(1/x)$$

For exp. $h(x) = h_3 x^3 + h_2 x^2 + h_1 x + h_0$

$$h(1/x) = \frac{h_3}{x^3} + \frac{h_2}{x^2} + \frac{h_1}{x} + h_0$$

$$h^*(x) = x^3 \left(\frac{h_3}{x^3} + \frac{h_2}{x^2} + \frac{h_1}{x} + h_0 \right)$$

$$= h_0 x^3 + h_1 x^2 + h_2 x + h_3$$

Exp. (7,4) Hamming code

$$h(x) = x^4 + x^2 + x + 1$$

$$h^*(x) = \cancel{1 + x^2 + x^3 + x^4}$$

$$= x^4\left(\frac{1}{x^4} + \frac{1}{x^2} + \frac{1}{x} + 1\right)$$

$$= \boxed{x^4 + x^3 + x^2 + 1}$$

The generator polynomial for dual code of (7,4) Hamming code.

$$x^3 + x^2 + 1$$

$$\boxed{x^4 + x^3 + x^2 + 1}$$

$$
\begin{array}{r}
x^7 + 1 \\
x^7 + x^6 + x^5 + x^3 \\
\hline
x^6 + x^5 + x^3 + 1 \\
x^6 + x^5 + x^4 + x^2 \\
\hline
x^4 + x^3 + x^2 + 1 \\
x^4 + x^3 + x^2 + 1 \\
\hline
\end{array}
$$

dual code $(7, 3)$ cyclic code.

$(H.W.)$

Conjecture! $(n, n-k)$??

$\nearrow n-k$ & $h(x)$ $\nearrow k$ are

Q. Suppose $g(x)$ ... the generator poly and parity-check poly for an (n,k) cyclic code.

Since cyclic code is also a linear code, what are the generator and the parity-check matrices?

$\underline{c}_{1\times n} = \underline{i}_{1\times k}\, G_{k\times n}$

$G = [\,I \mid \;]_{k\times(n-k)}$

$$g(x) = g_{n-k}\, x^{n-k} + g_{n-k-1}\, x^{n-k-1} + \dots + g_2 x^2 + g_1 x + g_0$$

$n-(n-k+1) = k-1$

$$G = \begin{bmatrix} g_{n-k} & g_{n-k-1} & \dots & g_2 & g_1 & g_0 & 0 & 0 & \dots & 0 \\ 0 & g_{n-k} & g_{n-k-1} & \dots & & g_1 & g_0 & 0 & \dots & 0 \\ 0 & 0 & g_{n-k} & \dots & & & g_1 & g_0 & \dots & 0 \\ & & & & & & & \dots & g_1 & g_0 \end{bmatrix}$$

$K \times n$

$K - m$ row

For exp.

$\vdots \quad 0 \quad 0 \quad 0 \cdots\cdots g_{n-K} \; g_{n-K-1} \cdots$

(7, 4) - Hamming.

$$g(x) = x^3 + x + 1$$

$$= g_3 x^3 + g_2 x^2 + g_1 x + g_0$$

$g_3 = 1$, $g_2 = 0$, $g_1 = 1$, $g_0 = 1$

$\bar{C}(x) = i(x) g(x)$

$$G = \begin{bmatrix} g_3 & g_2 & g_1 & g_0 & 0 & 0 & 0 \\ 0 & g_3 & g_2 & g_1 & g_0 & 0 & 0 \\ 0 & 0 & g_3 & g_2 & g_1 & g_0 & 0 \\ 0 & 0 & 0 & g_3 & g_2 & g_1 & g_0 \end{bmatrix}$$

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

$$h(x) = h_K x^K + h_{K-1} x^{K-1} + \dots + h_2 x^2 + h_1 x + h_0.$$

$$\boxed{H_{(n-K)\times n}}$$

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & \dots & h_{K-1} & h_K & 0 & \dots & 0 \\ 0 & h_0 & h_1 & h_2 & \dots & h_{K-1} & h_K & 0 \dots & 0 \\ \vdots & \vdots & \vdots & & & & \dots & h_K & 0 \\ 0 & 0 & h_0 & h_1 & \dots & & \dots & h_{K-1} & h_K \\ & & 0 & h_0 & h_1 & \dots & & & \\ 0 & \dots & & & & & & & \end{bmatrix}$$

(7,4) Hamming Code

Exp.

$$x^4 + x^2 + x + 1$$

$$u(n) = h_4 \quad h_3 \quad h_2 \quad h_1 \quad h_0$$

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & h_3 & h_4 & 0 & 0 \\ 0 & h_0 & h_1 & h_2 & h_3 & h_4 & 0 \\ 0 & 0 & h_0 & h_1 & h_2 & h_3 & h_4 \end{bmatrix}$$

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