

Double-error correcting BCH code

Bose, Chaudhuri-Hocquenghem

Binary Hamming code of length $n=2^m$; m parity checks

↓
corrects 1 error.

$$H = \begin{bmatrix} 1 & 2 & 3 & \dots & n \end{bmatrix}$$

↓ each column
 m tuple

• with $2m$ parity checks

↓
corrects 2 errors

$$H' = \begin{bmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{bmatrix}$$

↓ each column
 $2m$ tuple.

Example: $m=4, n=2^4=16$

$$H = \begin{bmatrix} 0000000011111111 \\ 000111100001111 \\ 001010100110011 \\ 011001001001001 \\ 101010101010101 \end{bmatrix}$$

or

$$H = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & \dots & 15 \end{bmatrix}$$

$$H' = \begin{bmatrix} 1 & 2 & \dots & 15 \\ f(1) & f(2) & \dots & f(15) \end{bmatrix}$$

↓ i th column

$$H_i = \begin{pmatrix} i \\ f(i) \end{pmatrix}$$

Let
2 errors occur

Syndrome

$$S = H_i + H_j$$

$$= \begin{pmatrix} i+j \\ f(i)+f(j) \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \text{ (say).}$$

$$\left. \begin{aligned} i+j &= z_1 \\ f(i)+f(j) &= z_2 \end{aligned} \right\} \text{ find } i, j \text{ given } z_1, z_2$$

• $i, j, f(i), f(j) \rightarrow$ all n -tuples
4-tuples.

$y \rightarrow$ received vector

$$S = H'y = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

~~need a field~~

- need to perform addition, subtraction, mul, div. with these n-tuples.
- need these n-tuples to be elements of a field.

How to construct such fields?

4-tuples

$GF(16)$

Galois field

$\rightarrow GF(2^4)$

$\rightarrow 16$ elements
binary

$x^{15} = 1$

$\downarrow$
each element, 4 tuple

$\downarrow$ each element polynomial of degree ≤ 3 .

power of x	4-tuple	polynomial
0	0 0 0 0	0
1	0 0 0 1	1
x	0 0 1 0	x
x ⁴	0 0 1 1	x + 1
x ²	0 1 0 0	x ²
x ⁸	0 1 0 1	x ² + 1
x ⁵	0 1 1 0	x ² + x
x ¹⁰	0 1 1 1	x ² + x + 1
x ³	1 0 0 0	x ³
x ¹⁴	1 0 0 1	x ³ + 1
x ⁹	1 0 1 0	x ³ + x
x ⁷	1 0 1 1	x ³ + x + 1
x ⁶	1 1 0 0	x ³ + x ²
x ¹³	1 1 0 1	x ³ + x ² + 1
x ¹¹	1 1 1 0	x ³ + x ² + x
x ¹²	1 1 1 1	x ³ + x ² + x + 1

$x^{10} = x + 1 + x^2$
 $x^4 = x + 1$
 $x^6 = x + x^2 + x^3$
 $x^7 = x^4 + x^3 = x + 1 + x^3$
 $x^{12} = x + 1 + x^2 + x^3$

modulo a poly of deg. 4.
 $\pi(x) = x^4 + x + 1$

$a_0 a_1 a_2 a_3$
 $+ b_0 b_1 b_2 b_3$
 $x^3 = x + 1 + x^2 + x^3$
 $x^4 = x + 1 + x^2 + x^3$
 $x^5 = x^4 + x$

addition - ok.

multiplication

$(1101) \cdot (1001)$
 $= (x^3 + x^2 + 1)(x^3 + 1)$
 $= x^6 + x^3 + x^5 + x^2 + x^3 + 1$
 $= x^6 + x^5 + x^2 + 1$

$\downarrow$
 want it to be an element of $GF(16)$
 i.e. a poly of deg ≤ 3 .

4-terms

$$(1101) \cdot (1001) = x^6 + x^4 + x + 1 \pmod{x^4 + x + 1}$$

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

$$= x^3 + x^2$$

$$= 1100$$

• Multiplication inverse exists if $\pi(x)$ is irreducible.

$$(1100)^{-1} = ?$$

$$1100 = x^3 + x^2 = x^6$$

$$= x^8 \cdot x^4 \cdot x^4 \cdot x^4 \cdot x^4 \cdot x^4 \cdot x^4 \cdot x^4$$

$$= x^{15} = x^6 \cdot x^9$$

$$x^4 \cdot x^2 = (x+1)x^2 = x^3 + x^2 = 1100$$

$$(1010)^{-1} = ?$$

$$1010 = x^3 + x = x^9$$

$$= x^6 = 1100$$

$$1 = x^{15} = x^9 \cdot x^6$$

Handwritten notes:
 $x^3 + x = x(x^2 + 1)$
 $x^2 + 1 = (x+1)^2$
 $x^3 + x = x(x+1)^2$
 $x^9 = x^3 \cdot x^3 \cdot x^3 = x(x+1)^2 \cdot x(x+1)^2 \cdot x(x+1)^2$
 $x^9 = x^3 \cdot x^3 \cdot x^3 = x^3 \cdot x^3 \cdot x^3 = x^3 \cdot x^3 \cdot x^3$

Square root

$$(0110)^{\frac{1}{2}} = (x^5)^{\frac{1}{2}} = (x^{15+5})^{\frac{1}{2}} = (x^{20})^{\frac{1}{2}} = x^{10} = 0111$$

② $\pi(x) = x^4 + x + 1 = 0$

x is a zero of $\pi(x)$. | cyclic group
 x is also a generator of $GF(16) \setminus \{0\}$.
 under multiplication as $x^{15} = 1$

primitive element $\rightarrow$ generator of a cyclic group.
 primitive polynomial $\rightarrow$ if a poly has a primitive element as zero.

• $\pi(x) = x^4 + x + 1 \rightarrow$ irreducible primitive poly as x is a zero of this poly when x generates the cyclic group $GF(16) \setminus \{0\}$ of order 15.

• $x \rightarrow$ primitive element.

$x^4 \rightarrow$ also primitive element.

• $x^3, x^5 \rightarrow$ not primitive element.

$$(x^3)^{15} = 1 \text{ but also.}$$

$$(x^3)^5 = 1 \text{ \& } 5 < 15 \Rightarrow x^3 \text{ not primitive element.}$$

Double error correcting BCH code

$$i+j = z_1$$

$$f(i) + f(j) = z_2$$

Choice of f : i) $f(i) = ci, c \text{ const.}$

$$\left. \begin{array}{l} i+j = z_1 \\ c(i+j) = z_2 \end{array} \right\} \text{ redundant, can't solve}$$

ii) $f(i) = i^2$

$$\left. \begin{array}{l} i+j = z_1 \\ i^2 + j^2 = z_2 \end{array} \right\} \text{ again redundant} \quad \text{i.e. } (i+j)^2 = z_2$$

(iii) $f(i) = i^3$

$$\begin{array}{l} i+j = z_1 \\ i^3 + j^3 = z_2 \end{array}$$

$$\begin{aligned}
 z_2 &= i^3 + j^3 = (i+j)(i^2 + ij + j^2) \\
 &= (i+j)((i+j)^2 - ij) \\
 &= z_1(z_1^2 + ij) \quad z_1 \neq 0
 \end{aligned}$$

$$\therefore ij = z_1^2 + \frac{z_2}{z_1}$$

~~(i, j)~~ $\rightarrow$ $i, j \rightarrow$ roots of the eqnⁿ

$$x^2 + z_1 x + \left(z_1^2 + \frac{z_2}{z_1}\right) = 0, z_1 \neq 0$$

no error $\Rightarrow z_1 = 0 = z_2$

Single error at location $i \Rightarrow S = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} i \\ i^3 \end{pmatrix}$.

Decoding strategy for double error - correcting BCH code

$y \rightarrow$ received vector

Compute syndrome

$$S = H^T y = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \text{ say}$$

i) if $z_1 = z_2 = 0 \rightarrow$ no error

ii) if $z_1 \neq 0, z_2 = z_1^3 \rightarrow$ Single error at location $i = z_1$
correct it

iii) if $z_1 \neq 0, z_2 \neq z_1^3 \rightarrow$ Construct eqnⁿ.

$$\textcircled{1} \quad x^2 + z_1 x + \left(z_1^2 + \frac{z_2}{z_1}\right) = 0.$$

$\downarrow$ find roots.

if 2 distinct roots exists, say, i, j , ~~correct~~ error
at these locations $\rightarrow$ correct them.

if $\textcircled{1}$ has no roots or if $z_1 = 0, z_2 \neq 0 \rightarrow$ detect at least

3 errors occurred.

Note.

① has to be solved in $GF(16)$ or $GF(2^m)$.

↓
4 tuple

↓
m tuple.

as $i, j, z_1, z_2 \rightarrow$ all elements of this field.

Parity check matrix for ~~2~~ Double-error correcting

BCH code

$$H = (H_1 H_2 \dots) \quad H_i = (i \text{cis}) = \begin{pmatrix} i \\ i^3 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix}$$

$\alpha^3 \rightarrow$ not primitive element

BCH code
of length $n=15$

$GF(2^4)$

generated by

16 elements.

↓
 α primitive

$$\alpha^{15} = 1$$

$GF(2^4) \setminus \{0\}$

$GF(2^m)$

↓
 α primitive
 $\alpha^{2^m - 1} = 1$

$$\therefore H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m - 2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^m - 2)} \end{pmatrix}$$

each column
2^m tuple.

↓
BCH code of length $n = 2^m - 1$

↓
 $GF(2^m) \setminus \{0\}$
= $\{ \alpha^1, \alpha^2, \dots, \alpha^{2^m - 2} \}$
2^m - 1 elements

Example:

Double error-correcting BCH code of length 15

• $GF(2^4)$ generated by $\boxed{\alpha^4 + \alpha + 1 = 0}$. $\alpha^5 = 1$

• Parity check matrix

$n = 2^4 - 1 = 15$
 $r = 8$
 $k = n - r = 7$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}$$

$$= \begin{pmatrix} \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{matrix} \\ \hline \begin{matrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{matrix} \\ \hline H_1 & H_2 & H_3 & H_4 & H_5 & H_6 & H_7 & H_8 & H_9 & H_{10} & H_{11} & H_{12} & H_{13} & H_{14} \end{pmatrix}$$

Example of decoding procedure

• Two errors at positions 6 & 8 say

i.e. in the columns $(\alpha^6, \alpha^3), (\alpha^8, \alpha^9)$

$$\therefore \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = H_6 + H_8 \Rightarrow \begin{matrix} \cancel{z_1 = 0011 + 0101 = 0111} \\ z_1 = 0011 + 1010 = 1001 \\ \quad \alpha^6 + \alpha^8 = \alpha^{14} \end{matrix}$$

$$z_2 = 0001 + 0101 = 0100$$

$$\begin{aligned} \frac{z_2}{z_1} + z_1^2 &= \alpha^2 + \alpha^{13} \\ &= 0010 + 1011 \\ &= 1001 \\ &= \alpha^{14} \end{aligned}$$

$$z_1^{-1} = \alpha \text{ as } \alpha^{15} = \alpha^{14} \cdot \alpha = 1$$

$$\therefore x^2 + z_1 x + \left(\frac{z_2}{z_1} + z_1^2 \right) = x^2 + \alpha^{14} x + \alpha^{14} = (x + \alpha^6)(x + \alpha^8)$$

∴ indeed the roots give the locations of the errors.

Three errors in places $1, 2, 4$ say.

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = H_1 + H_2 + H_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\Rightarrow z_1 = 1000 + 0010 +$$

$$\Rightarrow z_1 = 1000 + 0100 + 0001 = 1101 = \alpha^7$$

$$z_2 = 1000 + 0001 + 0101 = 1100 = \alpha^4$$

Then $x^2 + z_1 x + \left(\frac{z_2 + z_1^2}{z_1} \right) = x^2 + \alpha^7 x + \alpha^5$

~~this~~ has no zeros in the field $\Rightarrow$ at least 3 errors occurred.

$$\begin{aligned} \frac{z_2}{z_1} + z_1^2 &= \alpha^4 \alpha^8 + \alpha^{14} \\ &= \alpha^{12} + \alpha^{14} \\ &= 1111 + 0100 \\ &= 1011 \\ &= 0110 \\ &= \alpha^5 \end{aligned}$$

Theorem The double error correcting BCH code C has parameters $[n, k, 5]$, $m \geq 3$ as $t=2$

$[n=2^m-1, k=n-2m, 5]$, $m \geq 3$. C is cyclic code with generator polynomial

$$g(x) = M^{(1)}(x) M^{(3)}(x)$$

Example: The above BCH code of length 15 has generator polynomial

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

cyclic codes

$C \rightarrow$ i) linear

ii) any cyclic shift of a codeword is also a codeword

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

$\Downarrow$

$$a_{n-1} a_0 a_1 \dots a_{n-2} \in C$$

$$a_{n-2} a_{n-1} a_0 a_1 \dots a_{n-3} \in C$$

Example:

$$C_1 = \{0000, 0101, 1010, 1111\}$$

cyclic

$$\rightarrow C_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$C_2 = \{0000, 0110, 1001, 1111\}$$

not cyclic

$$\rightarrow C_2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$C_1 \sim C_2$$

$C_1, C_2 \rightarrow$ equivalent codes, but C_1 is cyclic, C_2 non cyclic

Note: A cyclic code may be equivalent to a non cyclic code.

$$C_1 = \{0000, 0101, 1010, 1111\}$$

$$\downarrow \quad \downarrow$$

$$0 \quad x+x^3$$

$$\underline{\underline{x^n = 1}}$$

Example:

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

$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$

$$0 \quad 1+x \quad 1+x^2 \quad x+x^2$$

$$x^0 c(x) = c_0 x^0 + c_1 x^1 + \dots + c_{n-1} x^{n-1} \pmod{x^n - 1}$$

$$= c_{n-1} + c_0 x + \dots + c_{n-2} x^{n-1}$$

$$\sim (c_{n-1}, c_0, c_1, \dots, c_{n-2})$$

$$c = (c_0, c_1, c_2, \dots, c_{n-1}) \in F^n$$

$$\leftrightarrow c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$$

$$\tilde{c} = (c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in F^n$$

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

• $F \rightarrow$ field

• $F[x] \rightarrow$ ring of polys. in x , co-efficient from the field F .

• $R_n = F[x]/(x^n - 1)$

$\rightarrow$ ring of polys. in x , of deg. $\leq n-1$, co-constants from the field F .

$\rightarrow$ vector space of dim n over F .

$$c(x) \in R_n \Rightarrow c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

$$\sim (c_0, c_1, \dots, c_{n-1})$$

$$xc(x) = xc_0 + c_1x^2 + \dots + c_{n-2}x^{n-1} + c_{n-1}x^n$$

$$\text{mod } (x^n - 1)$$

$$= c_0x + c_1x^2 + \dots + c_{n-2}x^{n-1} + c_{n-1}$$

$$\sim (c_{n-1}, c_0, c_1, \dots, c_{n-2})$$

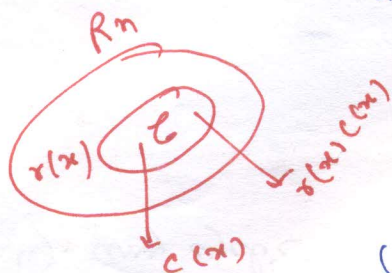
Then multiplying by x in R_n

$\Rightarrow$ a cyclic shift.

• $\mathcal{C} \rightarrow$ ideal of R_n if

i) $\mathcal{C}$ is linear subspace of R_n

ii) if $c(x) \in \mathcal{C}$ then $xc(x) \in \mathcal{C}$
 $\forall x(x) \in R_n$



or

(ii)' if $c(x) \in \mathcal{C}$
then $xc(x) \in \mathcal{C}$.

• A cyclic code of length n is an ideal of R_n

$\Rightarrow x^n c(x) \in \mathcal{C}, \dots, x^{n-1} c(x) \in \mathcal{C}$
 $\Rightarrow \sigma(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathcal{C}$
 starting $\mathcal{C}$

• $\mathcal{C} \rightarrow$ ideal in $R_n = F[x]/(x^n - 1)$
 i.e. $\mathcal{C} \rightarrow$ cyclic code of length n

a) $\exists$ unique monic poly $g(x)$ of minimal degree in $\mathcal{C}$

b) $\mathcal{C} = \langle g(x) \rangle$

c) $g(x)$ is a factor of $x^n - 1$

d) any $c(x) \in \mathcal{C}$ can be written as $c(x) = f(x)g(x)$
 in $F[x]$, where $f(x) \in F[x]$ has degree $< n-r$,
 $r = \deg g(x)$.

• dimension of $\mathcal{C}$ is $k = n-r$

• Thus $f(x) \in F[x]$ of $\deg < k$ becomes
 codeword $c(x) = f(x)g(x)$.

e) if $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_rx^r$, then $\mathcal{C}$ is
 generated by the rows of the generator matrix

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ & g_0 & g_1 & \dots & g_r & & & \\ & & & \dots & & & & \\ 0 & & & & g_0 & g_1 & \dots & g_r \end{bmatrix}_{(n-r) \times n}$$

$$= \begin{bmatrix} g(x) & & & \\ & x g(x) & & \\ & & \ddots & \\ & & & x^{n-r-1} g(x) \end{bmatrix}$$

a) uniqueness of $g(x)$

$f(x), g(x)$ monic, both having minimal degree r .
 $\in \mathcal{L}$.

$$\therefore f(x) - g(x) \in \mathcal{L} \rightarrow \deg. < r.$$

as $\mathcal{L}$ linear ($\rightarrow \mathcal{L}$)

b)

$$\mathcal{L} = \langle g(x) \rangle$$

$$\text{let } c(x) = q(x)g(x) + r(x) \text{ in } R_n$$

$$\deg r(x) < r.$$

$$r(x) = \underbrace{c(x)}_{\in \mathcal{L}} - \underbrace{q(x)g(x)}_{\in \mathcal{L}} \in \mathcal{L} \text{ as } \mathcal{L} \text{ is linear}$$

with $\deg r(x) < r$.
 $(\rightarrow \mathcal{L})$

$$\therefore r(x) = 0.$$

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

$$\text{or } \mathcal{L} = \langle g(x) \rangle$$

c) $g(x) \mid (x^n - 1)$

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

in $F[x]$

modulo $x^n - 1$

$$0 = q(x)g(x) + r(x) \text{ in } R_n.$$

$$r(x) = -q(x)g(x) \in \langle g(x) \rangle.$$

$$\Rightarrow r(x) \in \mathcal{L} \text{ by (b) } (\rightarrow \mathcal{L}) \text{ unless } r(x) = 0.$$

with $\deg r(x) < r$

$$\therefore g(x) \text{ is a factor of } x^n - 1.$$

(d) ^{any} $c(x) \in \mathcal{C}$, $\deg(c(x)) < n$

$$\therefore c(x) = q(x)g(x) \text{ in } R_n$$

$$\therefore c(x) = q(x)g(x) + h(x)(x^n - 1) \text{ in } F[x]$$

$$\begin{array}{l} \downarrow \\ \deg. < n \end{array} = q(x)g(x) + h(x)g(x)e(x) \quad \text{" } g(x)e(x) \text{ as } g(x) \mid x^n - 1$$

$$= g(x) (q(x) + h(x)e(x)) \text{ in } F[x].$$

$$= f(x)g(x) \text{ in } F[x]$$

$$\begin{array}{l} \swarrow \quad \downarrow \\ \deg. r. \end{array}$$

$$\deg f(x) < n - r.$$

(e) Thus $\mathcal{C} \rightarrow$ consists of ~~all~~ multiples of $g(x)$ by polynomials of degree $\leq n - r - 1$ in $F[x]$

$n - r$ linearly ind. multiples of $g(x)$

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

① $\downarrow$
rows of the generator matrix G of $\mathcal{C}$.
 $n - r \times n$

$\downarrow$
code has dimension $k = n - r$.

Parity Check matrix $x^n - 1 = g(x)h(x)$.

$g(x) \rightarrow$ generator polynomial of $\mathcal{C}$.

$$\downarrow \deg g(x) = r$$

$$\therefore \deg h(x) = n - r = k.$$

$$\text{let } h(x) = h_0 + h_1x + \dots + h_kx^k, \quad h_k \neq 0.$$

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

$$h(x) = \frac{x^n - 1}{g(x)} = \sum_{i=0}^k h_i x^i, h \neq 0 \text{ (say)}$$

→ check polynomial of $\mathcal{C}$.

any $c(x) \in \mathcal{C}$.

$$c(x) = f(x)g(x) = \sum_{i=0}^{n-1} c_i x^i$$

↓
deg $\leq n$

$$\therefore c(x)h(x) = \underbrace{f(x)g(x)}_{x^n - 1} h(x) = \sum_{i=0}^{n-1} c_i x^i \sum_{j=0}^k h_j x^j$$

$= 0 \text{ in } \mathbb{R}_{n^2} = \mathbb{F}[x]/(x^n - 1)$

coefficient of x^j

parity check $\textcircled{1}$ eqns.

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0, \quad j = 0, 1, \dots, n-1.$$

subscripts modulo n .

$$H = \begin{bmatrix} 0 & h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 \\ h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & x^{n-k} \overleftarrow{h(x)} & \dots & 0 \\ x^{n-k-1} \overleftarrow{h(x)} & \dots & \dots & 0 \end{bmatrix}$$

H is a parity check matrix for $\mathcal{C}$ as

- $\textcircled{1}$ says that if $c \in \mathcal{C}$ then $Hc^T = 0$.
- rows of H are lin. ind., $k = \deg h(x) = n - \deg(g(x)) = \dim \mathcal{C}$

• Example: find the generator matrix of all ternary codes of length 4.

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

$$= \cancel{(x^2 + 1)} \cancel{(x^2 + 1)} (x - 1)$$

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

$$F_3 = \mathbb{F}_3 = \{0, 1, 2\}$$

→ 3 factors
how many generator polys.
→ $3 \cdot 4 + 3 \cdot 2 = 12 + 6 = 18$
+1 = 19

Factors → 1, $1+x$, $2+x$, $1+x^2$, $(1+x)(2+x)$, $(1+x)(1+x^2)$

• $g(x) = 1$ $r=0$ $u = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ $(2+x)(1+x^2)$

• $g(x) = 1+x$ $r=1$ $u = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ $n=4$ $k=3$

$$g(x) = g_0 + g_1x + \dots + g_r x^r$$

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

$r=2$ $u = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ $n=4$ $k=2$

$r=3$ $u = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$ $n=4$ $k=1$

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

$r=3$ $u = \begin{pmatrix} 2 & 1 & 2 & 1 \end{pmatrix}$ $n=4$ $k=1$

• $g(x) = 1+x^2$ $r=2$ $u = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ $n=4$ $k=2$

• $g(x) = (1+x)(2+x)$ $u = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix}$ $n=4$ $k=2$

$r=2$ $n=4$ $k=2$

exmp: How many cyclic codes of length 6 over F_3 ?

$$\begin{aligned} x^6 - 1 &= (x^3 + 1)(x^3 - 1) \\ &= (x^3 + 1)(x^2 + 1)(x - 1) \\ &= (x^3 + 1)(x^2 + 1)(x + 1)(x + 2) \end{aligned}$$

$(x^3 + 1)^2 = x^6 + 2x^3 + 1 = x^6 + x^3 + 1$

$$\begin{aligned} x^6 - 1 &= (x^2)^3 - 1^3 = (x^2 - 1)(x^4 + x^2 + 1) \\ &= (x + 1)(x - 1)(x^2 + 1)^2 \\ &= (x + 1)(x - 1)(x^2 - 1)^2 \\ &= (x + 1)(x - 1)[(x + 1)(x - 1)]^2 \\ &= (x + 1)^3(x - 1)^3 \\ &= (x + 1)^3(x + 2)^3 \end{aligned}$$

6 factors.

of generator polys

$$\rightarrow 1 + C_1 + C_2 + \dots + C_5 = 2^6 - 1 = 63$$

Binary

Hamming code is cyclic

parity check matrix

$$H = [1 \quad \alpha \quad \alpha^2 \quad \dots \quad \alpha^{2^m - 2}]$$

each column

binary m-tuple

an element of $GF(2^m)$

excluding 0

let α be a primitive

element of $GF(2^m)$

Example $\mathcal{H}_3$

$$n = 2^3 - 1 = 7$$

$$H = (1 \ \alpha \ \alpha^2 \ \alpha^3 \ \alpha^4 \ \alpha^5 \ \alpha^6)$$

$$\alpha \in GF(2^3) \text{ satisfying } \alpha^3 + \alpha + 1 = 0.$$

$$C = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{H}_m \text{ iff } H C^T = 0$$

$$\text{iff } \sum_{i=0}^{n-1} c_i \alpha^i = 0.$$

$$\text{if } c(x) = 0$$

$$c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$$

$$c(x) = 0 \Rightarrow \text{minimal polynomial of } \alpha$$

$$M^{(1)}(x) \mid c(x).$$

$$\therefore \mathcal{H}_m = \mathcal{C}$$

$\Rightarrow \mathcal{H}_m$ is cyclic code with generator polynomial

$$g(x) = M^{(1)}(x)$$

$$H_{n-k \times n} = \begin{pmatrix} \overleftarrow{h(x)} \\ \alpha \overleftarrow{h(x)} \\ \vdots \\ \alpha^{k-1} \overleftarrow{h(x)} \end{pmatrix}$$

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

$$G = \begin{pmatrix} M^{(1)}(x) \\ x M^{(1)}(x) \\ \vdots \\ x^{k-1} M^{(1)}(x) \end{pmatrix}$$

• generator poly for double-error correcting BCH code.

• $M^{(i)}(x) \rightarrow$ minimal polynomial of α^i

• $M(x)$ is minimal poly. of $\alpha \in GF(p^m)$

$\Rightarrow M(x)$ is lowest degree monic poly.

having α as a zero.

i.e. $M(\alpha) = 0$, coefficients of $M(x)$ are from $GF(p)$.

$GF(p^m) \rightarrow p^m$ elements

$GF(p^m) \setminus \{0\} \rightarrow$ multiplicative cyclic group.
or order $p^m - 1$.

$\rightarrow$ has a generator / primitive element.

say α

$$\therefore \alpha^{p^m - 1} = 1, \quad \alpha \text{ non-zero.}$$

$$\Rightarrow \alpha^{p^m} = \alpha.$$

$\downarrow$
satisfied by $\alpha = 0$ also.

$\beta \in GF(p^m)$ satisfies $x^{p^m} - x = 0$.

$\downarrow$
monic polynomial.

β may satisfy a lower degree eqn.

$\downarrow$
 β is a ~~root~~ zero of this monic poly.

$\downarrow$
concept of minimal poly.

minimal poly. of $\beta \in GF(p^m)$

$\rightarrow$ lowest degree monic poly

have β as a zero.

Example

in $GF(2^4)$

mod $\pi(x) = x^4 + x + 1$

Element

0

1

α

monic poly

x

$1+x$

$1+x+x^4$

• Properties of minimal poly. $M(x)$ of $\beta \in GF(p^m)$

- $M(x)$ is irreducible
- $f(x)$ any poly. over $GF(p^m)$ has β as a zero
then $M(x) \mid f(x)$.

- $M(x) \mid x^{p^m} - x$.

- $\deg M(x) \leq m$.

- minimal poly. $M(x)$ of a primitive
element $\beta \in GF(p^m)$

has $\deg = m$.

$M(x) \rightarrow$ called primitive poly.

$\downarrow$

minimal poly of β when

β is ~~is~~ a generator
of $GF(p^m) \setminus \{0\}$

- β, β^p have the same minimal poly.
in $GF(2^m)$ β, β^2 have the same minimal poly.

• Double error correction BCH code $\rightarrow$ generator polynomial

• Computing minimal polynomials $\rightarrow$ Cyclotomic cosets

Properties of minimal poly. $M^{(i)}(x) \rightarrow$ Table for $GF(2^4)$.

properties of Minimal Polynomial of $\beta \in GF(p^m)$.

$M(x) \rightarrow$ minimal poly of β
lowest deg poly having β as a zero.

$M(x)$ irreducible

$f(\beta) = 0$, coefficients from $GF(p)$
then $M(x) \mid f(x)$

$M(x) \mid x^{p^m} - x$

$\deg M(x) \leq m$

$\deg M(x) = m \rightarrow$ primitive poly.
if β is a primitive element.

$\beta, \beta^p \rightarrow$ same minimal poly.

$M(x) = M_1(x)M_2(x) \neq 0$
 $\Rightarrow M_1(x) \neq 0$ or $M_2(x) \neq 0$
 $\Rightarrow \beta$ is a root of
either $M_1(x) \neq 0$ or
 $M_2(x) \neq 0$
($\rightarrow \leftarrow$)

$f(x) = M(x)q(x) + r(x)$
with $\deg r(x) < \deg f(x)$
At β
 $0 = 0 + r(\beta)$
($\rightarrow \leftarrow$) unless
 $r(x) \neq 0$.

Example:

$GF(2^4)$

$\alpha(x) = x^4 + x^3 + 1$

$\downarrow$

$\downarrow$

minimal poly of $\alpha \in GF(2^4)$.

$\alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^4)^2 = \alpha^8, (\alpha^8)^2 = \alpha^{16} = \alpha$

$\downarrow$

same minimal poly.

$\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^6)^2 = \alpha^{12}, (\alpha^{12})^2 = \alpha^{24} = \alpha^9, (\alpha^9)^2 = \alpha^{18} = \alpha^3$

$\downarrow$

same minimal poly.

powers $\rightarrow$ modulo 15

$GF(p^m)$ modulo $p^m - 1$.

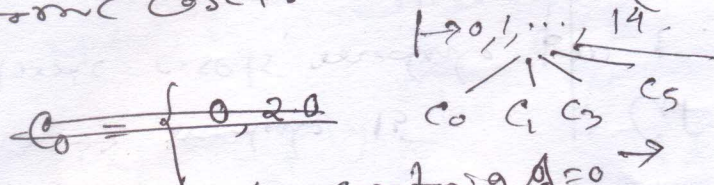
cyclotomic cosets modulo $p^m - 1$.

$\downarrow$
cyclotomic coset containing

$= \{ \alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, \dots, \alpha^{p^{m-1}} \}$

$m_p \rightarrow$ parallel to
int. set.
 $p^{m_p} \cdot \alpha \equiv \alpha \pmod{p^m - 1}$

• Cyclotomic cosets mod 15 ($p=2$).



Cyclotomic coset containing $\alpha=0 \rightarrow$

$$C_0 = \{0, 2, 4, \dots\} \quad 0, 2 \cdot 0 = 0 \quad C_0 = \{0\}.$$

multiplying α by p ~~the~~ modulo $p^m - 1$.

Cyclotomic coset containing $\alpha=1 \rightarrow 1, 2 \cdot 1 = 2, 2^2 \cdot 1 = 4, 2^3 \cdot 1 = 8, 2^4 \cdot 1 = 1$

$$C_1 = \{1, 2, 4, 8\}$$

Cyclotomic coset containing $\alpha=3 \rightarrow 3, 2 \cdot 3 = 6, 2^2 \cdot 3 = 12, 2^3 \cdot 3 = 24 = 9, 2^4 \cdot 3 = 18 = 3$

$$C_3 = \{3, 6, 12, 9\}$$

Cyclotomic coset containing $\alpha=5 \rightarrow 5, 2 \cdot 5 = 10, 2^2 \cdot 5 = 20 = 5$

$$C_5 = \{5, 10\}$$

Cyclotomic coset containing $\alpha=7 \rightarrow 7, 2 \cdot 7 = 14, 2^2 \cdot 7 = 28 = 13, 2^3 \cdot 7 = 26 = 11, 2^4 \cdot 7 = 22 = 7$

$$C_7 = \{7, 14, 13, 11\}$$

$C_p \rightarrow p$ is the smallest element in the coset, $p \rightarrow$ coset representative modulo $p^m - 1$.

• $M^{(i)}(\alpha) \rightarrow$ minimal poly of $\alpha^i \in GF(2^m)$.

$\therefore M^{(p^i)}(\alpha) = M^{(i)}(\alpha) \rightarrow$ minimal poly of $\alpha^i \in GF(2^m)$
 $\downarrow$
 minimal poly of $\alpha^{p^i} \in GF(2^m)$

example: $GF(2^4)$ defined by $\pi(x) = x^4 + x + 1$ $\pi(\alpha) = \alpha^4 + \alpha + 1 = 0$.

powers of α	polynomials	4 tuples	Minimal poly
$\alpha^0 = 1$	1	1 0 0 0	$x + 1$
$\alpha^1 \checkmark$	x	0 1 0 0	$M^{(1)}(x) = x + 1$
$\alpha^2 \checkmark$	x^2	0 0 1 0	$M^{(3)}(x)$
α^3	x^3	0 0 0 1	$M^{(7)}(x)$
$\alpha^4 \checkmark$	$x^4 = x + 1$	1 1 0 0	
α^5	$x^2 + x$	0 1 1 0	$M^{(5)}(x)$
$\alpha^6 \checkmark$	$x^3 + x^2$	0 0 1 1	
α^7	$x^4 + x^3 = x + 1 + x^3$	1 1 0 1	$M^{(7)}(x)$
α^8	$x^2 + x + x^4 = x^2 + x + x + 1 = x^2 + 1$	1 0 1 0	
$\alpha^8 \alpha^9$	$x^3 + x$	0 1 0 1	
$\alpha^9 \alpha^{10}$	$x^4 + x^2 = x + 1 + x^2$	1 1 1 0	
$\alpha^{10} \alpha^{11}$	$x^2 + x + x^3$	0 1 1 1	
$\alpha^{11} \alpha^{12}$	$x^3 + x^2 + x^4 = x^3 + x^2 + x + 1$	1 1 1 1	
α^{13}	$x^4 + x^3 + x^2 + x = x + 1 + x^3 + x^2 + x = 1 + x^2 + x^3$	1 0 1 1	
α^{14}	$x + x^3 + x^4 = x + x^3 + x + 1 = 1 + x^3$	1 0 0 1	
α^{15}	$x + x^4 = 1$		

$$M^{(1)}(x) = M^{(2)}(x) = M^{(4)}(x) = M^{(8)}(x)$$

$$M^{(3)}(x) = M^{(6)}(x) = M^{(12)}(x) = M^{(9)}(x)$$

$$M^{(7)}(x) = M^{(14)}(x) = M^{(13)}(x) = M^{(11)}(x)$$

$$M^{(5)}(x) = M^{(10)}(x)$$

• $M^{(1)}(x) \rightarrow$ minimal poly. of $\alpha^1 = \alpha$
 $= x^4 + x + 1$
 As α satisfies $\alpha^4 + \alpha + 1 = 0$.

• $M^{(3)}(x) \rightarrow$ has ~~α~~ α^3 as a zero.

let $M^{(3)}(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$.
 $\text{deg.} \leq 4$.

$$\therefore a_0 + a_1\alpha^3 + a_2\alpha^6 + a_3\alpha^9 + a_4\alpha^{12} = 0$$

$$a_0(1000) + a_1(0001) + a_2(0011) + a_3(0101) + a_4(1111) = 0$$

$$\begin{aligned} \alpha^4 &= \alpha + 1 \\ \alpha^5 &= \alpha^2 + \alpha \\ \alpha^6 &= \alpha^3 + \alpha^2 \\ &= 1000 + 0100 \\ &= 1100 \\ \alpha^9 &= \alpha^3 \cdot \alpha^6 \\ &= \alpha^3(\alpha^2 + \alpha) \\ &= \alpha^5 + \alpha^4 \\ &= \alpha^2 + \alpha + \alpha + 1 \\ &= \alpha^2 + 2\alpha + 1 \\ &= 0101 \end{aligned}$$

$$\Rightarrow \begin{aligned} a_0 + a_4 &= 0 & a_0 = a_1 = a_2 = a_3 = a_4 = 1 \\ a_3 + a_4 &= 0 \\ a_2 + a_4 &= 0 \\ a_1 + a_4 &= 0 \end{aligned}$$

$$M^{(3)}(x) = 1 + x + x^2 + x^3 + x^4$$

• $M^{(5)}(x) \rightarrow$ has α^5 as a zero

$$a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$$

$$\therefore a_0 + a_1\alpha^5 + a_2\alpha^{10} + a_3\alpha^{15} + a_4\alpha^{20} = 0$$

$$a_0(1000) + a_1(0110) + a_2(1110) + a_3(1000) + a_4(0110) = 0$$

$$\begin{aligned} a_0 + a_2 + a_3 &= 0 \\ a_1 + a_2 + a_4 &= 0 \\ a_1 + a_2 + a_4 &= 0 \end{aligned} \Rightarrow \begin{aligned} a_2 &= 1 \\ a_0 + a_3 &= 1 & a_0 = 1, a_3 = 0 \\ a_1 + a_4 &= 0 & a_1 = 1, a_4 = 0 \end{aligned}$$

$$M^{(5)}(x) = 1 + x + x^2$$

$$a_0 = a_1 = a_2 = 1, a_3 = a_4 = 0$$

$$\begin{aligned} \alpha^{12} &= \alpha^9 \cdot \alpha^3 \\ &= (\alpha^2 + \alpha) \cdot \alpha^3 \\ &= \alpha^5 + \alpha^4 \\ &= \alpha^2 + \alpha + \alpha + 1 \\ &= \alpha^2 + 2\alpha + 1 \\ &= 1111 \end{aligned}$$

$$M^{(7)}(x) \rightarrow \text{not zero.}$$

$$a_0 + a_1 x^7 + a_2 x^{14} + a_3 x^{21} + a_4 x^{28} = 0.$$

$$a_0 + a_1 x^7 + a_2 x^{14} + a_3 x^6 + a_4 x^{13} = 0.$$

$$a_0(1000) + a_1(1101) + a_2(1001) + a_3(0011) + a_4(1011) = 0.$$

$$a_0 + a_1 + a_2 + a_4 = 0 \Rightarrow a_0 + a_2 + a_4 = 0 \Rightarrow a_0 = a_4.$$

$$a_1 + a_3 = 0 \Rightarrow a_1 = 0 \quad a_3 = 1$$

$$a_3 + a_4 = 0 \Rightarrow a_3 = a_4.$$

$$a_1 + a_2 + a_3 + a_4 = 0 \Rightarrow a_1 = a_2 = 0.$$

$$M^{(7)}(x) = 1 + x^3 + x^4.$$

$$x^n - 1 = \prod_{d|n} M^{(d)}(x)$$

Double-error correcting BCH code of length $n = 2^m - 1$.

↓ parity check matrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^m-2)} \end{pmatrix}$$

$\alpha^{2^m-2} = \alpha^{2^m-1-1} = \alpha^{-1}$
 $\alpha^{3(2^m-2)} = \alpha^{3(2^m-1-1)} = \alpha^{-3}$

$$c \in \mathcal{C} \text{ iff } cH^T = 0$$

$$(c_0, c_1, \dots, c_{n-1}) \text{ iff } c_0 + c_1 \alpha + c_2 \alpha^2 + \dots + c_{n-1} \alpha^{n-1} = 0$$

$$\& c_0 + c_1 \alpha^3 + c_2 \alpha^6 + \dots + c_{n-1} \alpha^{3(n-1)} = 0.$$

$$\text{iff } c(\alpha) = 0 \& c(\alpha^3) = 0. \text{ iff } M^{(1)}(x) | c(x) \& M^{(3)}(x) | c(x).$$

$$M^{(d)}(x) = \prod_{i \in \mathcal{C}_d} (x - \alpha^i)$$

↓
Minimal poly of α^d
 $\mathcal{C}_d \rightarrow$ cyclotomic coset containing d
 $\text{LCF}(P_m) = \mathcal{C}_d$

$M^{(1)}(x) \rightarrow$ min. poly of α

$M^{(2)}(x) \rightarrow$ min. poly of α^2

$\therefore c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{C}$ iff $M^{(1)}(x) | c(x) \neq M^{(2)}(x) | c(x)$

$$c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$$

iff ~~$M^{(1)}(x)$~~ $\text{lcm} \{ M^{(1)}(x), M^{(2)}(x) \} | c(x)$
 $\downarrow \quad \downarrow$
irreducible irreducible

$$\therefore M^{(1)}(x), M^{(2)}(x) | c(x)$$

generator poly. of double-error correcting

$$\text{BCH code is } g(x) = M^{(1)}(x) M^{(2)}(x)$$

$$\downarrow$$
$$\left[n = 2^m - 1, \quad k = n - 2m, \quad d \geq 5 \right], m \geq 3$$

In general t -error correcting BCH code of length $2^m - 1$

Binary narrow sense
BCH code

generator polynomial

$$g(x) = \text{lcm} \{ M^{(1)}(x), M^{(2)}(x), \dots, M^{(2t)}(x) \}$$

~~deg $g(x) \geq 2t$~~

Example: 3 ~~3~~ - error correcting BCH code of

length ~~20~~ ~~21~~ $2^{16} - 1 = 15$

generator polynomial

GF(2^{16}).

module an irreducible

poly $f(x) = x^4 + x + 1$
 $g(x) = \text{lcm} \{ M^{(1)}(x), M^{(2)}(x), \dots, M^{(6)}(x) \}$. Minimal $\downarrow$
 primitive poly of d .

$= \text{lcm} \{ M^{(1)}(x), M^{(3)}(x), M^{(5)}(x),$ so $d^4 + d + 1 = 0$.

~~$M^{(7)}(x)$~~

$= M^{(1)}(x) M^{(3)}(x) M^{(5)}(x) \text{ ~~$M^{(7)}(x)$~~ }$

§

parity check matrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2^t} & \alpha^{2^{2t}} & \dots & \alpha^{2^t(n-1)} \end{pmatrix}$$

$$M^{(1)}(x) = x^4 + x + 1$$

$$M^{(3)}(x) = 1 + x + x^2 + x^3 + x^4$$

$$M^{(5)}(x) = 1 + x + x^2$$

$$d = 24 + 1$$

$$t = \frac{d-1}{2}$$

1-error corrector BCH code $\rightarrow$ Hamming code

2-error ~~3~~ $\dots$

3-error $\dots$

4-error $\dots$

5-error $\dots$

$$\textcircled{2} \quad \text{GF}(\mathbb{D}p^m) \setminus \{0\} = \langle \alpha \rangle$$

$$\alpha^{p^m - 1} = 1.$$

$$(x^{p^m} - 1) \rightarrow (x^{p^m} - x)$$

$$\alpha \left\{ \begin{array}{l} f(\alpha) = 0 \\ f'(\alpha) = 0 \end{array} \right.$$

(GF(p^m))

$$\textcircled{3} \quad \left(n^{n-1}, nx^{n-1} \right) = 1$$

$\text{gcd}(n, q) = 1.$

$$C_3 = \{3, 6, 12, 9\}.$$

$$M^{(3)}(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$$

$$= (x^2 + \alpha^2 x + \alpha^9) \times (x^2 + \alpha^8 x + \alpha^6)$$

$$= x^4 + x^3 (\alpha^8 + \alpha^2) + x^2 (\alpha^6 + \alpha^9 + \alpha^{10}) + x (\alpha^8 + \alpha^2) + \alpha^{15}$$

$$= x^4 + x^3 + x^2 + x + 1.$$

	0	1	2	3
$\alpha^3 =$	0	0	0	1
$\alpha^6 =$	0	0	1	1
$\alpha =$	0	0	1	0

$$\alpha^{12} = 1111$$

$$\alpha^9 = 0101$$

$$\alpha^8 = 1010$$

Example: Binary Hamming code $\mathcal{H}_m$ has parameters

$$[n=2^m-1, k=n-m, d=3], \text{ parity check}$$

$$\text{matrix } H = (1 \ \alpha \ \alpha^2 \ \dots \ \alpha^{2^m-2})$$

Where each entry is to be replaced by the corresponding column vector of m 0's & 1's.

e.g. for $\mathcal{H}_3$, the parity check matrix is

$$H = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$$

①

$$= \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \rightarrow \alpha^2 \\ \rightarrow \alpha \\ \rightarrow 1 \end{matrix}$$

When $\alpha \in GF(2^3)$ satisfies

$$\alpha^3 + \alpha + 1 = 0$$

$$\begin{aligned} \alpha^2 + \alpha &= \alpha \cdot \alpha^3 = \alpha^4 \\ \alpha^4 + \alpha^2 + 1 &= 0 \\ \alpha^5 &= \alpha^3 + \alpha^2 \\ &= \alpha + 1 + \alpha^2 \\ \alpha^6 &= \alpha^2 + \alpha + \alpha^3 \\ &= \alpha^2 + \alpha + \alpha + 1 \\ &= 1 + \alpha^2 \end{aligned}$$

Theorem The Hamming code $\mathcal{H}_m$ is a cyclic code with generator polynomial

$$g(x) = M^{(1)}(x).$$

Example:

for $\mathcal{H}_3$

$$n=7, m=3, k=4$$

$$g(x) = 1 + x + x^3 \leftrightarrow 1101$$

$\therefore \mathcal{H}_3$ has the generator matrix

$$A = \begin{pmatrix} g(x) & 0 & 0 & 0 \\ 0 & xg(x) & 0 & 0 \\ 0 & 0 & x^2g(x) & 0 \\ 0 & 0 & 0 & x^3g(x) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

• Rows of A are orthogonal to those of H .

- Let $\mathcal{C}$ be a cyclic code of length n with generator poly. $g(x)$.
Then $g(x) \mid x^n - 1$.

Then check polynomial $h(x) = \frac{x^n - 1}{g(x)}$.

Example: for the Hamming code $\mathcal{H}_3$ above, $n = 7$

$$h(x) = \frac{x^7 - 1}{1 + x + x^3}$$

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

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

Thus the parity check matrix is

$$H = \begin{pmatrix} 0 & \leftarrow h(x) \\ & \leftarrow xh(x) \\ & \leftarrow x^2h(x) & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

3×7

This is the same as ①.

Note: finding minimum distance d for a cyclic code $\rightarrow$ very difficult in general.

$$h(x) = \frac{x^n - 1}{g(x)} = \sum_{i=0}^k h_i x^i, \quad h_k \neq 0 \rightarrow \text{check poly. of } \mathcal{C}.$$

$$\text{for any } c(x) \in \mathcal{C}, \quad c(x) = \sum_{i=0}^{n-1} c_i x^i = f(x)g(x).$$

$$\therefore c(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) = 0 \text{ in } R_n = \frac{F[x]}{x^n - 1}$$

co-efficient of x^j

$$\textcircled{1} - \sum_{i=0}^{n-1} c_i h_{j-i} = 0, \quad j = 0, 1, \dots, n-1; \quad \text{subscripts modulo } n$$

parity check eqns.

$C \in \mathcal{C}$ must satisfy:

$$\textcircled{2} \begin{cases} C_{n-k-1} h_k + C_{n-k} h_{k-1} + \dots + C_{n-1} h_0 = 0 \\ C_{n-k-2} h_k + C_{n-k-1} h_{k-1} + \dots + C_{n-2} h_0 = 0 \\ \dots \\ C_0 h_k + C_1 h_{k-1} + \dots + C_k h_0 = 0. \end{cases}$$

i.e. C satisfies the linear recurrence

$$C_t h_k + C_{t+1} h_{k-1} + \dots + C_{t+k} h_0 = 0, \quad 0 \leq t \leq n-k-1.$$

Thus $C = \underbrace{(C_0 \quad C_1 \quad \dots \quad C_{n-k-1})}_{n-k \text{ check symbols.}} \underbrace{(C_{n-k} \quad \dots \quad C_{n-1})}_{k \text{ message symbols.}}$

↓
successively defined by eqn. $\textcircled{2}$.

The dual code

$\mathcal{C} \rightarrow$ a cyclic code with generator polynomial $g(x)$ & check polynomial $h(x) = \frac{x^n - 1}{g(x)}$

Theorem The dual code $\mathcal{C}^\perp$ is cyclic & has generator polynomial $g^\perp(x) = x^{\deg h(x)} h(x^{-1})$.

(if $h(x) = h_0 + h_1 x + \dots + h_k x^k$, then $g^\perp(x) = x^k (h_0 + \frac{h_1}{x} + \dots + \frac{h_k}{x^k})$
 $= h_k + h_{k-1} x + \dots + h_0 x^k$
 $\text{ref. } \left(\begin{matrix} g^\perp(x) & x g^\perp(x) & \dots & x^{n-k-1} g^\perp(x) \end{matrix} \right) = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 \\ h_k & h_{k-1} & \dots & h_0 \\ \dots & \dots & \dots & \dots \\ h_k & h_{k-1} & \dots & h_0 \end{pmatrix} \approx H_{n-k \times n}$

Thus the code with generator polynomial $h(x)$ is equivalent to $\perp$.

(Code words of $\perp$ written in backgrounds)

Exercise: Show that the $[7, 4, 3]$ code with $g(x) = x^3 + x + 1$ & the $[7, 3, 4]$ code with $g(x) = x^4 + x^3 + x^2 + 1$ are duals.

Hint. find check poly. $h(x)$ or to $g(x) = x^3 + x + 1$
Find reciprocal polynomial of $h(x)$.

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

$$h(x) = (1+x)(1+x^4+x^3)$$

$$= 1+x^4+x^3+x+x^5+x^4+x^3+x^2+x^6+x^5+x^4+x^3+x^2+x$$

$$= 1+x+x^4+0 \cdot x^3+x^4$$

reciprocal poly.

$$x^4+x^3+x^2+0 \cdot x+1 = x^4+x^3+x^2+1$$

factors of $x^n - 1$

cyclic code $\rightarrow$ ideal of $\langle q[x] \rangle$ $GF(q)/(x^n - 1)$
 $g(x) | (x^n - 1)$

- $GF(q)$, cyclic code, generator poly $| x^n - 1$.
- splitting field of $x^n - 1$??
- $n, q \rightarrow$ relatively prime (n odd if $q=2$)

- $m \rightarrow$ smallest integer s.t. $n | q^m - 1$. (such an integer always exists)

$\text{Ord}_n(q) \rightarrow$ multiplicative order of q modulo n .
 $s) q^m \equiv 1 \pmod{n}$
 $\rightarrow x^{n-1} | x^{q^m-1} - 1$, but does not divide $x^{q^l-1} - 1$ for $0 < l < m$.

$\rightarrow$ zeros of $x^n - 1$ lies in the extension field $GF(q^m)$.
 $\hookrightarrow n$ -th root of unity. if no smaller field.

- $x^n - 1 \rightarrow$ has n distinct zeros. (as $\gcd(x^n - 1, nx^{n-1}) = 1$)
 (gcd is 1 if $\gcd(n, q) \neq 1$)
 since $\gcd(n, q) = 1$

factoring $x^n - 1$ over $GF(q^m)$

- n distinct zeros (n -th roots of unity) of $x^n - 1 \rightarrow \alpha_0, \alpha_1, \dots, \alpha_{n-1} \in GF(q^m)$.

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha_i)$$

- $GF(q^m) \rightarrow$ splitting field of $x^n - 1$.

$$x^{q^m-1} - 1 = f(x)(x^n - 1)$$

$\Rightarrow$ zero of $(x^n - 1)$ is also a zero of $(x^{q^m-1} - 1)$ but not a zero of $(x^{q^l-1} - 1)$ for $0 < l < m$

$GF(q^m)$

zeros of $x^n - 1$

- Zeros of $x^n - 1$ form a cyclic subgroup of

$$GF(q^m)^*$$

i.e. $\exists$ an element $\alpha \in GF(q^m)$, called a primitive n -th root of unity, s.t.

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$$

- Zeros of $x^n - 1$ form the multiplicative group of a field iff $n = q^m - 1$

factoring of $x^n - 1$ over $GF(q)$

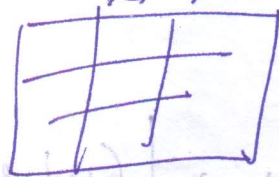
- the cyclotomic cosets mod $p^m - 1 \rightarrow$ already considered
- More generally, the cyclotomic coset mod n over $GF(q)$ consists of ~~s~~ containing s is

$$C_s = \{s, sq, sq^2, \dots, sq^{m_s-1}\}$$

where $sq^{m_s} \equiv s \pmod{n}$
(it is convenient but not essential to choose s to be the smallest integer in C_s).

- Then the integers mod n are partitioned into cyclotomic cosets:

$$\{0, 1, \dots, n-1\} = \bigcup C_s$$



partition of all integers mod n .

when s runs through a set of coset representatives mod n ,

e.g. for $n=9, q=2$

$$C_0 = \{0\}$$

$$C_1 = \{1, 2, 4, 8, 7, 5\}$$

$$C_3 = \{3, 6\}$$

$$\{1, q, q^2, \dots, q^{m-1}\}$$

At $q^m = 1$ mod n
 $\Rightarrow m$ is the smallest int. s.t.
 $n | q^m - 1$

$$GF(q^m)$$

Smallest extension
 containing all
 zeros
 of $x^n - 1$

$$x^n - 1 \mid x^{q^m} - 1$$

but $x^n - 1 \nmid x^{q^s} - 1$
 for $0 < s < m$.

- m = multiplication order of q
 modulo n $\hookrightarrow$ smallest integer
 $\leq m$ s.t. $m | q^m - 1$
 $= \# \text{ of } \alpha$ in C
 $= 6$.

- x^2 splits into linear factors
 over $GF(2^6)$.

Minimal poly. of α^i is

$$M^{(i)}(x) = \prod_{j \in C_i} (x - \alpha^j)$$

$\rightarrow$ monic poly. with
 c. coefficients from
 $GF(q)$

$\rightarrow$ lowest degree such
 poly. with α^i as a
 root.

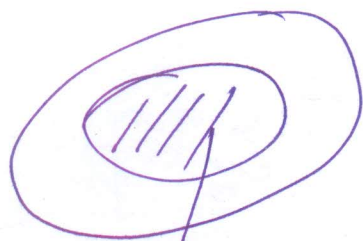
Also
$$x^n - 1 = \prod_s M^{(s)}(x)$$

When s runs through a set of coset representatives
 mod n .

- This is the factorization of $x^n - 1$ into irreducible polys.
 over $GF(q)$.

e.g. $n=9, q=2$
 when $M^{(0)}(x) = x+1$, $M^{(1)}(x) = x^6 + x^3 + 1$, $M^{(3)}(x) = x^2 + x + 1$
 $= (x - \alpha^0)$ $= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^5)$ $= (x - \alpha^3)(x - \alpha^6)$

$\mathcal{C} = \langle g(x) \rangle$, $g(x) \mid x^n - 1$ over $GF(q)$.
 $\downarrow$
 length n .



$GF(q^m)$
 smallest extension field

$m \rightarrow$ smallest +ve integer s.t.

$\downarrow$ all zeros of $x^n - 1$
 (i.e. n -th roots of unity)

$\downarrow$ cyclic subgroup of $GF(q^m)^*$

$n \mid q^m - 1$

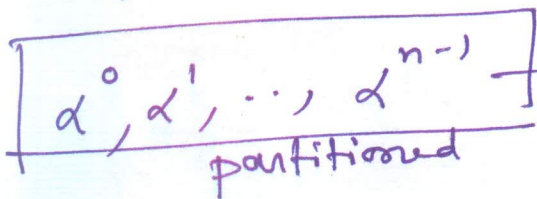
$\downarrow \langle \alpha \rangle$
 generator, called primitive
 n -th root of unity.

$\downarrow n = q^m - 1$
 cyclic gr. $GF(q^m)^*$

$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i) \rightarrow$ no distinct roots if n, q relatively prime.

$\prod_{i=0}^{n-1} (x - \alpha^i)$

$\rightarrow$ factoring of $x^n - 1$ over $GF(q^m)$
 splitting field of $x^n - 1$.

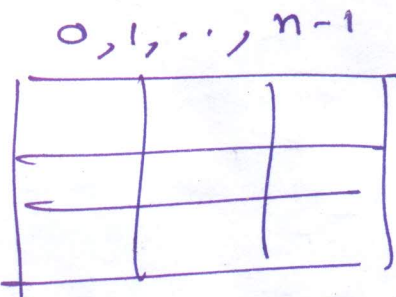


powers are partitioned into cyclotomic cosets modulo n .

$|C_i| = m$

$M(x)$

Minimal poly of $\alpha^i \in GF(q^m)$



C_s

over $GF(q) \rightarrow M^{(i)}(x) = \prod_{i \in C_s} (x - \alpha^i)$ coefficients from $GF(q)$

$x^n - 1 = \prod M^{(i)}(x)$, s runs over cyclotomic cosets modulo n
 $\hookrightarrow$ factorization of $x^n - 1$ into irreducible poly over $GF(q)$.

The Zeros of a Code.

$\alpha \rightarrow$ primitive n th root of unity

- $\mathcal{C} \rightarrow$ a cyclic code with generator poly. $g(x)$.
- $g(x) \mid x^n - 1$ over $\text{GF}(\alpha)$.
- $\therefore g(x) = \prod_{i \in K} (x - \alpha^i)$, $K =$ a union of cyclotomic cosets

The n th roots of unity $\{\alpha^i \mid i \in K\}$ are called the ~~the~~ zeros of the code.

- The other n th roots of unity $\{\alpha^i \mid i \notin K\}$ are called the non-zeros — these are zeros of check poly. $h(x) = \frac{x^n - 1}{g(x)}$

- if $c(x) \in R_n = \mathbb{F}[x]/(x^n - 1)$ then $c(x) \in \mathcal{C}$ iff $c(\alpha^i) = 0 \forall i \in K$.
($c(x) = f(x)g(x)$ & $g(\alpha^i) = 0$)

i.e. a cyclic code is defined in terms of the zeros of $c(x)$.

Exercise if $h(x) = \prod_{i \notin K} (x - \alpha^i)$ is a divisor of $x^n - 1$

over $\text{GF}(\alpha)$, then $\deg h(x) = n - |K|$ $h(\alpha^{-1}) = \text{const.} \prod_{i \notin K} (x - \alpha^{-i})$

$$g^\perp(x) =$$

- The zeros of the dual code are the inverses of the non-zeros of the original code.

Other generators

- $g(x) \rightarrow$ generator poly of a cyclic code $\mathcal{C}$
- $\rightarrow$ the lowest degree monic polynomial in the code.

Lemma 1 If $p(x) \in R_n$ does not introduce any new zeros, i.e. $p(\alpha^i) \neq 0$ for all $i \in K$, then $g(x)$ & $p(x)g(x)$ generate the same code. (e.g. $g(x)^2$ generates the same code as $g(x)$).

Proof clearly,

$$\langle g(x) \rangle \supseteq \langle p(x)g(x) \rangle \quad \text{--- (1)}$$

→ any element generated by $p(x)g(x)$ can be treated as generated by $g(x)$.

Now as $h(x), p(x)$ are relatively prime, $\exists a(x), b(x)$ by division algm. such that

$$1 = a(x)p(x) + b(x)h(x) \quad \text{in } F[x]$$

$$p(x)g(x) \in \langle g(x) \rangle$$

$$\Rightarrow \langle p(x)g(x) \rangle \subseteq \langle g(x) \rangle$$

$$p(x), h(x) \text{ coprime}$$

$$\therefore 1 = a(x)p(x) + b(x)h(x) \text{ in } F[x]$$

$$g(x) = a(x)p(x)g(x) + b(x)g(x)h(x) \text{ in } R_n$$

$$\Rightarrow \langle g(x) \rangle \subseteq \langle p(x)g(x) \rangle$$

$$\therefore \langle g(x) \rangle \subseteq \langle p(x)g(x) \rangle \quad \text{--- (2)}$$

→ $g(x)$ itself is a multiple of $p(x)g(x)$ → any element generated by $g(x)$ can be treated as generated by $p(x)g(x)$.

Combining (1) & (2), the lemma follows.

Lemma 2

Let $\xi \in GF(q^m)$ be any zero of $x^n - 1$.

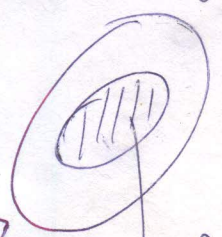
Then

$$\sum_{i=0}^{n-1} \xi^i = \begin{cases} 0 & \text{if } \xi \neq 1 \\ n & \text{if } \xi = 1 \end{cases}$$

Proof

$$\text{if } \xi = 1, \text{ then } \sum_{i=0}^{n-1} \xi^i = n$$

$$\text{if } \xi \neq 1, \text{ then } \sum_{i=0}^{n-1} \xi^i = \frac{1 - \xi^n}{1 - \xi} = 0 \text{ as } \xi \text{ is a zero of } x^n - 1$$



$GF(q^m)$
m divides n
inf. A.T.
 $n | q^m - 1$

zeros of $x^n - 1$
= n th roots of unity

Lemma 3

An inversion formula:

The vector $c = (c_0, c_1, \dots, c_{n-1})$

may be recovered from $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ by

$$c_i = \frac{1}{n} \sum_{j=0}^{n-1} c(\alpha^j) \alpha^{-ij}$$

Proof

$$\sum_{j=0}^{n-1} c(\alpha^j) \alpha^{-ij} = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} c_k \alpha^{j(k-i)} = \sum_{k=0}^{n-1} c_k \sum_{j=0}^{n-1} \alpha^{j(k-i)} = nc_i \text{ by lemma 2}$$

(α → primitive n-th root of unity)

→ α^i an element of $GF(q^m)$ of order n and a zero of $x^n - 1$

t-error correcting BCH code

Theorem
• (BCH bound)

Let $\mathcal{C} \rightarrow$ a cyclic code with generator polynomial $g(x)$
st. for some integer $b \geq 0, \delta \geq 1$

$$g(\alpha^b) = g(\alpha^{b+1}) = \dots = g(\alpha^{b+\delta-2}) = 0.$$

i.e. the code has a string of $\delta-1$ consecutive powers of α as a zero.

Then min. distance of the code is at least δ .

proof

If $c = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$ then

$$c(\alpha^b) = c(\alpha^{b+1}) = \dots = c(\alpha^{b+\delta-2}) = 0.$$

so that $H'c^T = 0$ where

$$H' = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \dots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix}$$

each row is a parity check

$$\begin{aligned} c_0 + c_1 \alpha^b + \dots + c_{n-1} \alpha^{(n-1)b} &= 0 \\ c_0 + c_1 \alpha^{b+1} + \dots + c_{n-1} \alpha^{(n-1)(b+1)} &= 0 \\ \vdots & \\ c_0 + c_1 \alpha^{b+\delta-2} + \dots + c_{n-1} \alpha^{(n-1)(b+\delta-2)} &= 0 \end{aligned}$$

(Note that H' need not be the full parity check matrix of $\mathcal{C}$)

Claim: Any $\delta-1$ or fewer columns of H' are linearly independent over $GF(q^m) \Rightarrow$ min. dist of the code is δ .

• if not, let $c \in \mathcal{C}$ has wt. $w \leq \delta-1$ i.e. $c_i \neq 0$ iff $i \in \{a_1, a_2, \dots, a_w\}$.

$$\text{Then } H'c^T = 0 \Rightarrow \begin{pmatrix} \alpha^{a_1 b} & \dots & \alpha^{a_w b} \\ \alpha^{a_1 (b+1)} & \dots & \alpha^{a_w (b+1)} \\ \vdots & \ddots & \vdots \\ \alpha^{a_1 (b+\delta-2)} & \dots & \alpha^{a_w (b+\delta-2)} \end{pmatrix} \begin{pmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_w} \end{pmatrix} = 0$$

$$\Rightarrow \begin{vmatrix} \alpha^{a_1 b} & \dots & \alpha^{a_w b} \\ \alpha^{a_1 (b+1)} & \dots & \alpha^{a_w (b+1)} \\ \vdots & & \vdots \\ \alpha^{a_1 (b+w-1)} & \dots & \alpha^{a_w (b+w-1)} \end{vmatrix} = 0.$$

$H \rightarrow$ parity check matrix
min. dist. d iff every
 $d-1$ cols. of H are lin.
ind. & some d cols
are lin. dep.

$$\text{i.e. } \alpha^{(a_1 + \dots + a_w) b} \begin{vmatrix} 1 & \dots & 1 \\ \alpha^{a_1} & \dots & \alpha^{a_w} \\ \vdots & & \vdots \\ \alpha^{a_1 (w-1)} & \dots & \alpha^{a_w (w-1)} \end{vmatrix} = 0. \quad (\rightarrow \Leftarrow).$$

$\swarrow$
Vandermonde determinant so nonzero

Example: The binary Hamming code $\mathcal{H}_m$ has generator polynomial $M^{(1)}(x)$

Now $M^{(1)}(\alpha) = M^{(1)}(\alpha^2) = 0$, so the code has a pair of consecutive zeros, α & α^2 .

$\therefore$ Minimum distance is ≥ 3

Example: The binary double-error correcting BCH code has $g(x) = M^{(1)}(x) M^{(3)}(x)$.

Now $M^{(1)}(\alpha) = M^{(1)}(\alpha^2) = M^{(1)}(\alpha^4) = 0$ & $M^{(3)}(\alpha^3) = 0$.

Thus there are 4 consecutive zeros: $\alpha, \alpha^2, \alpha^3, \alpha^4$.

hence the min. distance is ≥ 5 .

Min. dist. $> d$, for more than $d-1$ columns of H' may be linearly independent when the entries are replaced by m -tuples from $GF(q)$.

Corollary A cyclic code of length n with zeros $\alpha^b, \alpha^{b+r}, \alpha^{b+2r}, \dots, \alpha^{b+(d-2)r}$ where $r \neq n$ are relatively prime, has min. dist. at least d .

Proof. Let $\beta = \alpha^r$.
 Since r is relatively prime to n , β is also a primitive
 n th root of unity.

$\therefore \alpha^b = \beta^t$ for some t , if the code has zeros

$$\alpha^b = \beta^t, \beta^{t+1}, \dots, \beta^{t+b-2} \text{ i.e. } \alpha^{b+r}, \alpha^{b+2r}, \dots, \alpha^{b+(b-2)r}$$

Hence by ~~Theorem~~ BCH bound, min. dist. $\geq \delta$

BCH codes

A cyclic code of length n over $GF(q)$ is a BCH code
 of designated distance δ if, for some integer $b \geq 0$

$$g(x) = \text{l.c.m.} \{ M^{(b)}(x), M^{(b+1)}(x), \dots, M^{(b+\delta-2)}(x) \}$$

i.e. $g(x)$ is the lowest degree monic polynomial over
 $GF(q)$ having $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$ as zeros.

Therefore, c is in the code iff $c(\alpha^b) = c(\alpha^{b+1}) = \dots = c(\alpha^{b+\delta-2}) = 0$.

Thus the code has a string of $\delta-1$ consecutive
 powers of α as zeros.

Hence, by the BCH bound, min. dist. $\geq \delta$, the
 designated distance δ .

Parity Check matrix for the code is

$$H =_{m(\delta-1) \times n} \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \dots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix}$$

When each entry is replaced by the corresponding column of m elements from $GF(q)$.

$$\deg M^{(i)}(x) \leq m, \text{ then } \Rightarrow \deg g(x) = n - \dim \text{ of code} \leq m(d-1)$$

$$\Rightarrow \dim \text{ of code} \geq n - m(d-1).$$

Theorem A BCH code over $GF(q)$ of length n & designated distance δ has min. dist. $d \geq \delta$, and dimension $\geq n - m(d-1)$.

(When m is the multiplicative order of q modulo n i.e. m is the smallest integer s.t. $n \mid q^m - 1$)

The dimension will be greater than $n - m(d-1)$ if some of the rows of the $GF(q)$ version of H are linearly dependent, or (equivalently) if the degree of l.c.m. of $M^{(b)}(x), M^{(b+1)}(x), \dots, M^{(b+d-2)}(x)$ is less than $m(d-1)$.

1. Narrow sense BCH code (if $b=1$)

If $n = q^m - 1$, then α is a primitive element of the field $GF(q^m)$ (and not merely a primitive n -th root of unity). The code is called primitive code.

If some α^i is a zero of the code, then so are all α^l , for l in the cyclotomic coset C_i .

Since the cyclotomic cosets are smallest if $n = q^m - 1$, this is the most important case.

2. Nested BCH codes (if b is fixed).

- the code with designated distance δ_1 contains the code of designated distance δ_2 iff $\delta_1 \leq \delta_2$

3. In general, the dual of a BCH code is not a BCH code.

Binary BCH codes when $q=2$, $M^{(2i)}(x) = M^{(i)}(x)$,

and so the degree of $g(x)$ can be reduced.

for example if $b=1$, we may always assume that the designated distance δ is odd. for the codes with designated distance $2t$ and $2t+1$ coincide - both have

$$g(x) = \text{l.c.m. of } M^{(1)}(x), M^{(3)}(x), \dots, M^{(2t-1)}(x)$$

(Then $\deg g(x) \leq mt$ and the dimension of the code is $\geq n - mt$).

(The parity check matrix is

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t-1} & \dots & \dots & \alpha^{(2t-1)(n-1)} \end{pmatrix}$$

where each entry is replaced by the corresponding binary m -tuple.

2nd. column of H need only contain $\alpha, \alpha^{i_1}, \alpha^{i_2}, \dots$ where $i_1, i_2, \dots$ are in different cyclotomic cosets.

examples: (Narrow sense primitive binary BCH code)
of length 15 & 31.

BCH codes of length 15 $\rightarrow (1, \alpha, \alpha^2, \dots, \alpha^{14})$ $\alpha^{15} = 1$

designated distance δ	generator poly. $g(x)$	exponents of roots of $g(x)$	dim. $= n - \deg g(x)$	actual distance d
1	1	—	15	1
3	$M^{(1)}(x)$	1, 2, 4, 8	11	3
5	$M^{(1)}(x) M^{(3)}(x)$	1, 2, 4, 8, 9, 12	7	5
7	$M^{(1)}(x) M^{(3)}(x) M^{(5)}(x)$	1, 2, 4, 8, 9, 12, 10, 14	5	7
9, 11, 13 or 15 (Base dist = 15)	$M^{(1)}(x) M^{(3)}(x) M^{(5)}(x) M^{(7)}(x)$ $= (x^{15} + 1) / (x + 1)$	1-14	1	15

3 errors
BCH code
of length 15

BCH codes of length 31

δ	$g(x)$	exponents of roots of $g(x)$	dim. $= n - \deg g(x)$	true min. distance d
1	1	31	31	1
3	$M^{(1)}$		26	3
5	$M^{(1)} M^{(3)}$		21	5
7	$M^{(1)} M^{(3)} M^{(5)}$		16	7
9 or 11 (Base dist = 11)	$M^{(1)} M^{(3)} M^{(5)} M^{(7)}$		11	11
13 or 15 (Base dist = 15)	$M^{(1)} M^{(3)} M^{(5)} M^{(7)} M^{(9)}$		6	15
17, 19, ..., 31 (Base dist = 31)	$M^{(1)} M^{(3)} M^{(5)} M^{(7)} M^{(9)} M^{(11)} M^{(13)}$		1	31

Note that the codes of designated distance 9 & 11 coincide. Because the code with designated distance 11 has generator polynomial

$$g(x) = \text{l.c.m.} \{ M^{(1)}(x), M^{(3)}(x), M^{(5)}(x), M^{(7)}(x), M^{(9)}(x) \}$$

But $9 \in C_5$, so the minimal polys of α^9 & α^5 are the same: $M^{(5)}(x) = M^{(9)}(x)$.

$\therefore g(x) = \text{l.c.m.} \{ M^{(1)}(x), M^{(3)}(x), M^{(5)}(x), M^{(7)}(x) \}$
which is also the generator poly. of the code with designated distance 9.

Thus

- BCH code of designated distance δ may coincide with a BCH code of designated distance δ' , where $\delta' > \delta$.
- largest such δ' is called the Bose distance of the code.
- from the BCH bound, the true min. distance is at least equal to δ' , but may be greater.

Example: (The binary (nonprimitive) BCH codes of length $n=23$. ($n \neq 2^m-1$))

δ	$g(x)$	dim.	true min dist. d
1	1	23	
3 or 5 (Bose dist = 5)	$M^{(1)}$	12	
7, 9, ..., 23	$M^{(1)} M^{(5)}$	1	

(7) > designated distance δ
23

So the BCH bound is not tight.

The cyclotomic cosets are

$$C_0 = \{0\}$$

$$C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$$

$$C_5 = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}$$

Since $|G| = 11$, the multiplicative order of 23 mod 23 is $m = 11$.

So $x^{23} + 1$ splits into linear factors over $GF(2^{11})$ & α is a primitive 23^{rd} root of unity in $GF(2^{11})$.

Over $GF(2)$, $x^{23} + 1 = (x+1) M^{(1)}(x) M^{(5)}(x)$.

where $M^{(1)}(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$

$M^{(5)}(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$.

The BCH code with designated distance 5 ($\delta = 1$) has generator poly.

$$g(x) = \text{l.c.m.} \{M^{(1)}(x), M^{(3)}(x)\}$$

But $M^{(1)}(x) = M^{(3)}(x)$.

$\therefore g(x) = M^{(1)}(x)$ & the parity check matrix is

$$H = (1, \alpha, \alpha^2, \dots, \alpha^{22})$$

where each entry is replaced by a binary column of length 11.

- The dimension of the code is $23 - \deg g(x) = 12$
- Bose distance ~~is~~ is also 5
- This BCH code is equivalent to the Crokey code G_{23} & has min. distance 7, illustrating BCH bound is not tight.

prim 0, 1, 2, ..., 22 mod 23

$$C_0 = \{0\}$$

$$C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$$

$$C_5 = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}$$

$$\begin{array}{r} 1024 \\ 2048 \\ \hline 2048 \end{array}$$

$$1 = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = 3$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} + \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix} + \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} = 7$$

$$= 1 + 23 + 23 \cdot \frac{11}{2} + 23 \cdot \frac{22}{2} = 23[1 + 11 + 22] = 23 \cdot 34 = 782$$

perfect, triple error correcting code