ECE 405/511
Error Control Coding

Minimal Polynomials and BCH Codes

Minimal Polynomials

- Let α be an element of GF(q^m)
- The minimal polynomial of α with respect to GF(q) is the smallest degree monic (non-zero) polynomial

$$p(x) \text{ in GF}(q)[x]$$

  such that $p(\alpha) = 0$
  - The degree of $p(x)$ is d and $d|m$
  - $f(\alpha) = 0$ implies $p(x)|f(x)$
  - $p(x)$ is irreducible in GF(q)[x]
  - If α is a primitive element in GF(q^m), $p(x)$ is a primitive polynomial

- What are the other roots of $p(x)$?
  - The conjugates of α:

$$\{\alpha, \alpha^{q}, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}\}$$

  - This set of conjugates (with d elements) is called the conjugacy class of α with respect to GF(q)
  - All the roots of an irreducible polynomial have the same order so all elements of a conjugacy class have the same order

Example: GF(8)

let α be a root of $x^3+x+1 \longrightarrow q = 2$, $m = 3$ and $d|3$

conjugacy class	minimal polynomial
$\{0\}$	x
$\{1\}$	$x+1$
$\{\alpha, \alpha^2, \alpha^4\}$	$(x+\alpha)(x+\alpha^2)(x+\alpha^4) = x^3+x+1$
$\{\alpha^3, \alpha^6, \alpha^5\}$	$(x+\alpha^3)(x+\alpha^6)(x+\alpha^5) = x^3+x^2+1$

- Note that the roots are in GF(8), but the minimal polynomials have coefficients in the ground field GF(2)
- Same as multiplying by the conjugate polynomial in the complex field to obtain real coefficients

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

- Multiplying all the minimal polynomials of the non-zero elements of GF(8) gives

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

GF(16) formed from x^4+x+1

Power of α	Polynomial in α	Vector
$-\infty$	0	0000
0	1	1000
1	α	0100
2	α^2	0010
3	α^3	0001
4	$\alpha+1$	1100
5	$\alpha^2+\alpha$	0110
6	$\alpha^3+\alpha^2$	0011
7	$\alpha^3+\alpha+1$	1101
8	α^2+1	1010
9	$\alpha^3+\alpha$	0101
10	$\alpha^2+\alpha+1$	1110
11	$\alpha^3+\alpha^2+\alpha$	0111
12	$\alpha^3+\alpha^2+\alpha+1$	1111
13	$\alpha^3+\alpha^2+1$	1011
14	α^3+1	1001

- GF(16) = GF(2^4) $q = 2$, $m = 4$, $d|4$

  let α be a root of x^4+x+1

conjugacy class	order	minimal polynomial
$\{0\}$	-	x
$\{1\}$	1	$x+1$
$\{\alpha,\alpha^2,\alpha^4,\alpha^8\}$	15	x^4+x+1
$\{\alpha^3,\alpha^6,\alpha^{12},\alpha^9\}$	5	$x^4+x^3+x^2+x+1$
$\{\alpha^5,\alpha^{10}\}$	3	x^2+x+1
$\{\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}\}$	15	x^4+x^3+1

Cyclotomic Cosets

- The partition of powers of α by the conjugacy classes is called the set of cyclotomic cosets

- GF(8): {0}, {1,2,4}, {3,6,5}
- GF(16): {0}, {1,2,4,8}, {3,6,12,9}, {5,10}, {7,14,13,11}
- GF(32): {0}, {1,2,4,8,16}, {3,6,12,24,17}, {5,10,20,9,18}, {7,14,28,25,19}, {11,22,13,26,21}, {15,30,29,27,23}

Cyclotomic Cosets

- GF(32) = GF(2^5) let α be a root of x^5+x^2+1

cyclotomic coset	minimal polynomial
{0}	$M_0(x) = x+1$
{1,2,4,8,16}	$M_1(x) = x^5+x^2+1$
{3,6,12,24,17}	$M_3(x) = x^5+x^4+x^3+x^2+1$
{5,10,20,9,18}	$M_5(x) = x^5+x^4+x^2+x+1$
{7,14,28,25,19}	$M_7(x) = x^5+x^3+x^2+x+1$
{11,22,13,26,21}	$M_{11}(x) = x^5+x^4+x^3+x+1$
{15,30,29,27,23}	$M_{15}(x) = x^5+x^3+1$

- The generator polynomials of cyclic codes are
  - products of irreducible polynomials
  - factors of x^n-1

  so they are a product of minimal polynomials
- Therefore, one can look at cyclic codes in terms of the roots of the generator polynomial $g(x)$

Binary Cyclic Hamming Codes

- If $g(x)$ is a primitive polynomial of degree m over GF(2), then the ring of polynomials modulo $g(x)$, GF(2)[x]/$g(x)$, is the finite field of order 2^m.
- If α is a root of $g(x)$, then $\{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}$ are the 2^m elements of the field. Each element can also be represented by a binary m-tuple.
- Use the 2^m-1 non-zero elements to construct the columns of a matrix

$$\mathbf{H} = [\ 1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^{2^m-2}]$$

- The code C with parity check matrix **H** is a Hamming code with $n = 2^m$-1 as **H** contains all distinct non-zero m-tuples.

- Since $\mathbf{cH}^T = 0$, we can express the set of codewords as

$$C = \{c_0 c_1 \cdots c_{n-1} \mid c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0\}$$

$\rightarrow$ $c(x)$ has root α since $c(\alpha) = 0$

- As $g(\alpha) = 0$, $c(x)$ is a multiple of $g(x)$
  - therefore $c(x)$ is a codeword in the cyclic code generated by $g(x)$ and C is this cyclic code
- All binary Hamming codes are equivalent to cyclic codes
- Example: $g(x) = x^3+x+1 \rightarrow \mathrm{GF}(2)[x]/g(x)$ is GF(8)

  The field elements are

$\{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1\}$

$$\mathbf{H}=\begin{bmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{bmatrix}=[\mathbf{I}\;\;\mathbf{P}^{T}]$$

$$1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6$$

$$\mathbf{G}=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\1&1&1&0&0&1&0\\1&0&1&0&0&0&1\end{bmatrix}=\left[\mathbf{P}\;\mathbf{I}\right]$$

or

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

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

BCH Codes

- B – Bose
  C – Ray-Chaudhuri
  H – Hocquenghem
- BCH codes are a generalization of cyclic Hamming codes
  - $g(x)$ is a primitive polynomial
  - $c(\alpha) = 0$ if α is a root of $g(x)$
  - the corresponding parity check matrix has columns corresponding to powers of α from α^0 to α^{n-1} or all 2^m-1 distinct non-zero binary vectors of length m for a binary code

- Example: q = 2, m = 4

  $n = 2^m - 1 = 15$

  Consider the parity check matrix with columns arranged in increasing integer label order

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & & 1 \\ 0 & 1 & 1 & & 1 \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & \cdots & 15 \end{bmatrix}$$

- To generalize to 2 error correction, more rows need to be added to **H**. Add 4 more rows to **H** to get **H**'

$$\mathbf{H}' = \begin{bmatrix} 1 & 2 & 3 & \ldots & 15 \\ f(1) & f(2) & f(3) & \ldots & f(15) \end{bmatrix}$$

How to choose $f(i)$?

- Suppose 2 errors have occurred in positions *i* and *j*
- The syndromes are $\mathbf{S} = \mathbf{eH}^T = h_i + h_j$

$$S_1 = i+j,\ S_2 = f(i)+f(j)$$

- Require a function *f* such that S_1 and S_2 can be used to get *i* and *j*
  - try $f(i) = i^2$

    $S_2 = i^2+j^2 = (i+j)^2 = S_1^2 \longrightarrow$ no unique solution in GF(16)

- Next try $f(i) = i^3$

  $i+j = S_1$

  $i^3+j^3 = S_2$

  $S_2 = (i+j)(i^2+ij+j^2) = S_1(S_1{}^2+ij)$

  $\longrightarrow ij = S_2/S_1 + S_1{}^2$

- Now i and j are roots of the equation

  $\Lambda(x) = (x+i)(x+j) = x^2 + S_1x + S_2/S_1 + S_1{}^2$

  Error Locator Polynomial

Decoding Procedure

1. Compute the syndromes
2. Form the Error Locator Polynomial $\Lambda(x)$
3. Find the roots of $\Lambda(x)$
4. Flip the bits in the error positions

Double Error Correction Decoding

- Calculate the syndromes S_1 and S_2
  - if $S_1 = S_2 = 0$, no error
  - if $S_1 \neq 0$ and $S_2 = S_1^3$, 1 error at position *i*
  - if $S_1 \neq 0$ and $S_2 \neq S_1^3$, solve for the roots of the error locator polynomial
    - if there are 2 distinct roots *i* and *j*, correct the errors at these locations
    - if no roots, 1 root or a double root, do nothing as more than 2 errors have been detected
  - if $S_1 = 0$, $S_2 \neq 0$, more than 2 errors have been detected

- To obtain a cyclic code, place the columns of **H** in increasing powers of α

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \cdots & \alpha^{3(2^m-2)} \end{bmatrix}$$

- For the GF(16) example

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \cdots & \alpha^{12} \end{bmatrix}$$

- Now a codeword must satisfy

$$\mathbf{c}\mathbf{H}^{\mathrm{T}} = 0$$

$$\rightarrow c(\alpha) = 0,\ c(\alpha^3) = 0$$

- Therefore $g(x) = M_1(x)M_3(x)$

- The two error correcting BCH codes have parameters $(2^m\text{-}1, 2^m\text{-}1\text{-}2m, 5)$, $m > 3$

- Example:

  $m = 4$, $n = 15$, $k = 7$, $d = 5$ (15,7,5) BCH code

  $M_1(x) = x^4+x+1$

  $M_3(x) = x^4+x^3+x^2+x+1$

  $g(x) = M_1(x)M_3(x) = x^8+x^7+x^6+x^4+1$

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

$$
\mathbf{H} = \left[\begin{array}{ccccccccccccccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
\hline
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1
\end{array}\right]
$$

GF(16) formed from x^4+x+1

Power of α	Polynomial in α	Vector
-	0	0000
0	1	1000
1	α	0100
2	α^2	0010
3	α^3	0001
4	$\alpha+1$	1100
5	$\alpha^2+\alpha$	0110
6	$\alpha^3+\alpha^2$	0011
7	$\alpha^3+\alpha+1$	1101
8	α^2+1	1010
9	$\alpha^3+\alpha$	0101
10	$\alpha^2+\alpha+1$	1110
11	$\alpha^3+\alpha^2+\alpha$	0111
12	$\alpha^3+\alpha^2+\alpha+1$	1111
13	$\alpha^3+\alpha+1$	1011
14	α^3+1	1001

(15,7,5) BCH Code Example 1

- **r** = 110111101011000   arithmetic in GF(16)

  $r(x) = 1+x+x^2+x^3+x^4+x^5+x^6+x^8+x^{10}+x^{11}$

  The syndromes are

$$\mathbf{S} = \begin{bmatrix} S_1 \\ S_3 \end{bmatrix} = \begin{bmatrix} r(\alpha) \\ r(\alpha^3) \end{bmatrix} = \begin{bmatrix} \alpha^{11} \\ \alpha^5 \end{bmatrix}$$

The error locator polynomial is $\Lambda(x) = x^2 + \alpha^{11}x + 1$

  roots are α^7 and α^8

  r = 110111101011000

  e = 000000011000000

  c' = 110111110011000

(15,7,5) BCH Code Example 2

- arithmetic in GF(16)
- **r** = 100000001000000

  $r(x) = 1 + x^8$

  $S_1 = r(\alpha) = 1 + \alpha^8 = \alpha^2$ $S_3 = r(\alpha^3) = 1 + \alpha^{24} = \alpha^7$

  The error locator polynomial is

$$\Lambda(x) = x^2 + S_1 x + S_3 / S_1 + S_1^2 = x^2 + \alpha^2 x + \alpha^8$$

- To find the roots of the error locator polynomial, substitute powers of α to find the error locations

$$x = \alpha^0 = 1 \longrightarrow 1+\alpha^2+\alpha^8 = 0$$

there is an error in the 1st position

Since $x^2 + \alpha^2 x + \alpha^8 = (x+1)(x+\alpha^8)$

there is also an error in the 9th position

- What about correcting an arbitrary number of errors?

$$\mathbf{H} = \begin{bmatrix} \alpha^i \\ f_1(\alpha^i) \\ f_2(\alpha^i) \\ \vdots \end{bmatrix}$$

$$g(x) = M_1(x)M_3(x)\ldots$$

- If each additional function $f_j(x)$ is chosen appropriately we should be able to correct an additional error for each function added
- One choice can be determined using

  Vandermonde matrices

Vandermonde Matrices

$$\mathbf{V} = \begin{bmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \cdots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \cdots & \lambda_n^2 \\ \lambda_1^3 & \lambda_2^3 & \lambda_3^3 & \cdots & \lambda_n^3 \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda_1^n & \lambda_2^n & \lambda_3^n & \cdots & \lambda_n^n \end{bmatrix}_{n\times n} \qquad \lambda_i \in GF(q^m)$$

Theorem: If $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ are distinct non-zero elements of GF(q^m), then the columns of **V** are linearly independent over GF(q^m).

Let $\lambda_i = \alpha^{i-1}$, α an element of order n in GF(q^m)

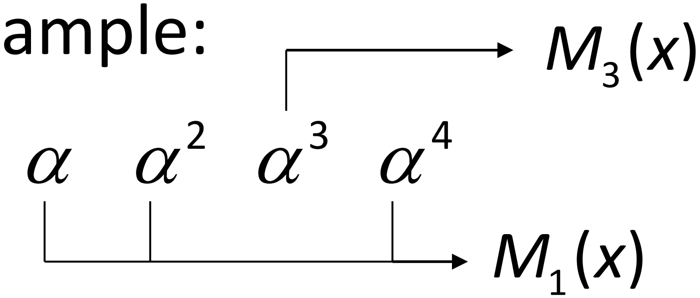
$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{3(n-1)} \\ \vdots & & & & \\ 1 & \alpha^{2t} & \alpha^{4t} & \ldots & \alpha^{2t(n-1)} \end{bmatrix}_{2t \times n}$$

$\alpha, \alpha^2, \cdots, \alpha^{2t}$ are roots of $g(x)$

Any $2t$ columns are linearly independent

$$\therefore \quad d > 2t$$

- GF(2^m) example:



If α is a zero of $g(x)$, so is α^2 and α^4

Therefore, for d = 5, only the rows

$$1 \quad \alpha \quad \alpha^2 \cdots \quad \alpha^{n-1}$$

$$1 \quad \alpha^3 \quad \alpha^6 \cdots \quad \alpha^{3(n-1)}$$

are required as previously shown. Redundant rows can be removed. The number of rows determines *n*-*k* so we want to minimize this number.

Theorem – BCH Bound

Let C be an (n,k) q-ary cyclic code with generator polynomial $g(x)$.

Let α be an element of order n in GF(q^m), $n | q^m$-1. If $g(x)$ is the monic polynomial of smallest degree such that

$$\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$$

are among its roots, then C has minimum distance at least δ. $g(x)$ is the product of the minimal polynomials of the roots

$$g(x) = \text{LCM}\{M_b(x), M_{b+1}(x), \ldots, M_{b+\delta-2}(x)\}$$

- δ is called the design distance (typically $2t+1$)
- The most commonly encountered BCH codes are the

  $n = q^m-1$ primitive (α is a primitive element of $GF(q^m)$)

  $b = 1$ narrow-sense

  BCH codes
- For any m and $t < n/2$, there exists a binary primitive BCH code with parameters

  $n = 2^m-1$, $d \geq 2t+1$, $n-k \leq mt$ →

  product of t minimal polynomials of degree m or less

- For q = 2, every second row in **H** can be deleted as α^{2i} has the same minimal polynomial as α^i
- Binary BCH code examples:

  $d = 3$ $(2^m\text{-}1, 2^m\text{-}1\text{-}m, 3)$ cyclic Hamming code

  $g(x) = M_1(x)$

  $d = 5$ $(2^m\text{-}1, 2^m\text{-}1\text{-}2m, 5)$

  $g(x) = M_1(x)M_3(x)$

Construction of BCH Codes

- To construct a t error correcting q-ary BCH code of length n:
  - Find an element α of order n in GF(q^m) where m is minimal, i.e. $n | q^m-1$
  - Select $2t$ consecutive powers of α starting with α^b
  - Find $g(x)$, the LCM of the minimal polynomials for these powers of α

Example: Binary BCH Codes of Length 31

- $q = 2$ and $n = 31 = 2^5 - 1$ so $m = 5$
- Let α be a root of x^5+x^2+1
- The cyclotomic cosets modulo 31 are

		Minimal polynomial	
c_0	{0}	$x+1$	$M_0(x)$
c_1	{1,2,4,8,16}	x^5+x^2+1	$M_1(x)$
c_3	{3,6,12,24,17}	$x^5+x^4+x^3+x^2+1$	$M_3(x)$
c_5	{5,10,20,9,18}	$x^5+x^4+x^2+x+1$	$M_5(x)$
c_7	{7,14,28,25,19}	$x^5+x^3+x^2+x+1$	$M_7(x)$
c_{11}	{11,22,13,26,21}	$x^5+x^4+x^3+x+1$	$M_{11}(x)$
c_{15}	{15,30,29,27,23}	x^5+x^3+1	$M_{15}(x)$

- Narrow-sense $b = 1$

t	roots of $g(x)$	$g(x)$	code
1	α,α^2	$M_1(x)$	(31,26,3)
2	$\alpha,\alpha^2,\alpha^3,\alpha^4$	$M_1(x)M_3(x)$	(31,21,5)
3	$\alpha,\alpha^2,\alpha^3,\ldots,\alpha^6$	$M_1(x)M_3(x)M_5(x)$	(31,16,7)
4	$\alpha,\alpha^2,\alpha^3,\ldots,\alpha^8$	$M_1(x)M_3(x)M_5(x)M_7(x)$	(31,11,11)

Note: for $t = 4$, $g(x)$ actually has 10 consecutive powers of α as roots, thus $d = 11$.

Binary BCH Codes with $b = 0$

- $b = 0 \longrightarrow$ start with $\alpha^0 = 1$
- For t error correction $2t$ roots of $g(x)$: $1, \alpha, \alpha^2, \ldots, \alpha^{2t\text{-}1}$
- $g(x)$ has $x+1$ as a factor
- d is even $\longrightarrow d \geq 2t+2$
- roots of $g(x)$: $1, \alpha, \alpha^2, \ldots, \alpha^{2t\text{-}1}, \alpha^{2t}$

conjugate of root α^t

Example: GF(8)

- $t = 1$, $2t = 2$, $b = 0$: 1 and α are the roots

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

  $= x^4+x^3+x^2+1$ $\qquad d = 4 > 2t+1$

- (7,3,4) cyclic code
  - dual of (7,4,3) Hamming code
- $h(x) = x^3+x^2+1$

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

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

$$h(x) = x^3+x^2+1 \qquad h^*(x) = x^3+x+1$$

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

GF(64) Minimal Polynomials

{0}	$x+1$	$M_0(x)$
{1,2,4,8,16,32}	x^6+x+1	$M_1(x)$
{3,6,12,24,48,33}	$x^6+x^4+x^2+x+1$	$M_3(x)$
{5,10,20,40,17,34}	$x^6+x^5+x^2+x+1$	$M_5(x)$
{7,14,28,56,49,35}	x^6+x^3+1	$M_7(x)$
(9,18,36}	x^3+x^2+1	$M_9(x)$
{11,22,44,25,50,37}	$x^6+x^5+x^3+x+1$	$M_{11}(x)$
{13,26,52,41,19,38}	$x^6+x^4+x^3+x+1$	$M_{13}(x)$
{15,30,60,57,51,39}	$x^6+x^5+x^4+x^2+1$	$M_{15}(x)$
{21,42}	x^2+x+1	$M_{21}(x)$
{23,46,29,58,53,43}	$x^6+x^5+x^4+x+1$	$M_{23}(x)$
{27,54,45}	x^3+x+1	$M_{27}(x)$
{31,62,61,59,55,47}	x^6+x^5+1	$M_{31}(x)$

Primitive BCH Codes of Length 63

(63,57,3)	(63,51,5)	(63,45,7)
(63,39,9)	(63,36,11)	(63,30,13)
(63,24,15)	(63,18,21)	(63,16,23)
(63,10,27)	(63,7,31)	

Non-primitive BCH Codes

- Example $n = 21$, $q = 2$ $m = ?$

  $n | 2^m - 1$ $m = 6$ (minimal) so use GF(64)
- Let α be a primitive element in GF(64)

  Let $\beta = \alpha^3$ so that $\beta^{21} = \alpha^{63} = 1$
- For $t = 2$ roots are $\beta, \beta^2, \beta^3, \beta^4 \longrightarrow \alpha^3, \alpha^6, \alpha^9, \alpha^{12}$

  $g(x) = (x^6+x^4+x^2+x+1)(x^3+x^2+1)$

  $= x^9+x^8+x^7+x^5+x^4+x+1$

  (21,12,5) non-primitive BCH code

- If $g(x)$ generates a cyclic code of length 21, it must be a factor of $x^{21}+1$
- Check:

$$x^{21}+1=(x+1)(x^2+x+1)(x^3+x+1)(x^3+x^2+1)(x^6+x^4+x^2+x+1)(x^6+x^5+x^4+x^2+1)$$

- There are many cases where the actual minimum distance is greater than the design distance
- Example: construct a BCH code with n = 23

  $23 | 2^{11}-1 \longrightarrow GF(2^{11})$ $2^{11}-1 = 23 \times 89$
- Let α be a primitive element in $GF(2^{11})$
- $\beta = \alpha^{89}$ so that $\beta^{23} = \alpha^{89 \times 23} = 1$
  - t = 1: required roots are β, β^2
  - adding the conjugates, the roots are:

    $\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^{32} = \beta^9,\beta^{18},\beta^{13},\beta^3,\beta^6,\beta^{12}$

  $g(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$
- design distance is 5: code parameters are (23,12,7)

(23,12,7) Cyclic Golay Code

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

GF(256) Cyclotomic Cosets

{0}	$M_1(x)$	{37,41,73,74,82,146,148,164}	$M_{37}(x)$
{1,2,4,8,16,32,64,128}	$M_1(x)$	{39,57,78,114,147,156,201,228}	$M_{39}(x)$
{3,6,12,24,48,96,129,192}	$M_3(x)$	{43,86,89,101,149,172,178,202}	$M_{43}(x)$
{5,10,20,40,65,80,130,160}	$M_5(x)$	{45,75,90,105,150,165,180,210}	$M_{45}(x)$
{7,14,28,56,112,131,193,224}	$M_7(x)$	{47,94,121,151,188,203,229,242}	$M_{47}(x)$
(9,18,33,36,66,72,132,144}	$M_9(x)$	{53,77,83,106,154,166,169,212}	$M_{53}(x)$
{11,22,44,88,97,133,176,194}	$M_{11}(x)$	{55,110,115,155,185,205,220,230}	$M_{55}(x)$
{13,26,52,67,104,134,161,208}	$M_{13}(x)$	{59,103,118,157,179,206,217,236}	$M_{59}(x)$
{15,30,60,120,135,195,225,240}	$M_{15}(x)$	{61,79,122,158,167,211,233,244}	$M_{61}(x)$
{17,34,68,136}	$M_{17}(x)$	{63,126,159,207,231,243,249,252}	$M_{63}(x)$
{19,38,49,76,98,137,152,196}	$M_{19}(x)$	{85,170}	$M_{85}(x)$
{21,42,69,81,84,138,162,168}	$M_{21}(x)$	{87,93,117,171,174,186,213,234}	$M_{87}(x)$
{23,46,92,113,139,184,197,226}	$M_{23}(x)$	{91,107,109,173,181,182,214,218}	$M_{91}(x)$
{25,35,50,70,100,140,145,200}	$M_{25}(x)$	{95,125,175,190,215,235,245,250}	$M_{95}(x)$
{27,54,99,108,141,177,198,216}	$M_{27}(x)$	{111,123,183,189,219,222,237,246}	$M_{111}(x)$
{29,58,71,116,142,163,209,232}	$M_{29}(x)$	{119,187,221,238}	$M_{119}(x)$
{31,62,124,143,199,227,241,248}	$M_{31}(x)$	{127,191,223,239,247,251,253,254}	$M_{127}(x)$