

ELEC 405

Error Control Coding and Sequences

Minimal Polynomials and BCH Codes

Minimal Polynomials

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

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

such that $p(\alpha) = 0$

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

- What are the other roots of $p(x)$?
 - The conjugates of α :
$$\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{d-1}}\}$$
 - This set of conjugates (with d elements) is called the **conjugacy class** of α with respect to $\text{GF}(q)$
 - 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 $x^3+x+1 \rightarrow q = 2, m = 3$ 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

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

- Multiplying all the minimal polynomials over GF(8) (except x) together 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	Vector
-	0	0000
0	1	1000
1	x	0100
2	x^2	0010
3	x^3	0001
4	$x+1$	1100
5	x^2+x	0110
6	x^3+x^2	0011
7	x^3+x+1	1101
8	x^2+1	1010
9	x^3+x	0101
10	x^2+x+1	1110
11	x^3+x^2+x	0111
12	x^3+x^2+x+1	1111
13	x^3+x+1	1011
14	x^3+1	1001

- $\text{GF}(16) = \text{GF}(2^4)$ $q = 2, m = 4, d \mid 4$

let α be a root of $1+x+x^4$

Conjugacy class	order	minimal polynomials
$\{0\}$	-	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): $\{0\}, \{1,2,4,8,16\}, \{3,6,12,24,17\},$
 $\{5,10,20,9,18\}, \{7,14,28,25,19\},$
 $\{11,22,13,26,21\}, \{15,30,29,27,23\}$

- The generator polynomials of cyclic codes are
 - products of irreducible polynomials
 - factors of x^n-1so they are a product of some minimal polynomials
- Therefore, one could look at cyclic codes in terms of the roots of $g(x)$.

Cyclic Hamming Codes

- If $g(x)$ is a primitive polynomial of degree m over $\text{GF}(2)$, the ring of polynomials modulo $g(x)$, $\text{GF}(2)[x]/g(x)$, is the field of order 2^m .
- Let α be a root of $g(x)$, then $\{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m-2}\}$ 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

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

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

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

$$\mathbf{C} = \{c_0c_1 \cdots c_{n-1} \mid c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0\}$$

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

- As $g(\alpha) = 0$, $c(x)$ is a multiple of $g(x)$
 - therefore $c(x)$ is a cyclic code.
 - all binary Hamming codes are equivalent to cyclic codes.
- Example: $g(x) = x^3+x+1 \rightarrow \text{GF}(2)[x]/g(x)$ is $\text{GF}(8)$
 The field elements are
 $\{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1\}$

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

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

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

or

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

BCH Codes

- B – Bose
C – Ray-Chaudhuri
H – Hocquenghem
- Binary 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 all non-zero powers of α or all distinct non-zero m -tuples

- Example: $m = 4$

$$n = 2^m - 1 = 15$$

Consider the parity check matrix with columns arranged in decimal order

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

- To generalize to 2 error correction, more rows need to be added to \mathbf{H} . Add 4 more rows to \mathbf{H} to get \mathbf{H}' .

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

How to choose $f(i)$?

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

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

- Suppose 2 errors have occurred in positions i and j
- The syndromes are $\mathbf{S} = \mathbf{h}_i + \mathbf{h}_j$

$$S_1 = i+j, S_2 = f(i)+f(j)$$
- How to find f such that we can solve S_1 and S_2 to get i and j ?
 - try $f(i) = i^2$

$$S_2 = i^2 + j^2 = (i+j)^2 = S_1^2 \quad \text{no unique solution in GF(16)}$$

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

$$i+j = S_1$$

$$i^3+j^3 = S_2$$

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

$$\Rightarrow ij = S_2/S_1 + S_1^2$$

- 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. find the roots of the error locator polynomial
 3. flip the bits in the error positions
- if there are no errors $S_1 = S_2 = 0$
 - if there is one error at position i , $S_2 = i^3 = S_1^3$

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 \mathbf{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

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

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

- Now a codeword must satisfy

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

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

- Therefore $g(x) = m_1(x)m_3(x)$

- The two error correcting BCH code parameters are $(2^m-1, 2^m-1-2m, 5)$
- Example:
 $m = 4, n = 15, k = 7, d = 5$ (15,7,5) BCH code

$$m_1(x) = x^4 + x + 1$$

$$m_3(x) = x^4 + x^3 + x^2 + x + 1$$

$$g(x) = m_1(x)m_3(x) = x^8 + x^7 + x^6 + x^4 + 1$$

- Suppose $\mathbf{r} = (110111101011000)$

The syndromes are

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

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

roots are α^7 and α^8

$$\mathbf{r} = 110111101011000$$

$$\mathbf{e} = 000000011000000$$

$$\mathbf{c}' = 110111110011000$$

Another Example

- $\mathbf{r} = 1000000001000000$ $n = 15$ GF(16)

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

$$\mathbf{S} = (S_1 S_2 S_3 S_4) = (\alpha^2, \alpha^4, \alpha^7, \alpha^8)$$

$$S_1 = r(\alpha) = \alpha^2 \quad S_2 = r(\alpha^2) = \alpha^4 = S_1^2$$

$$S_3 = r(\alpha^3) = \alpha^7 \quad S_4 = r(\alpha^4) = \alpha^8 = S_1^4$$

– so for binary codes, we only need to compute S_1 and S_3 .

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

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

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?

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

$$g(x) = m_1(x)m_3(x)\dots$$

- 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

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

Theorem: If $\lambda_1 \lambda_2 \lambda_3 \dots \lambda_n$ are distinct non-zero elements of $GF(q)$, then the columns of \mathbf{V} are linearly independent over $GF(q)$.

Let $\lambda_i = \alpha^{i-1}$, α a primitive element

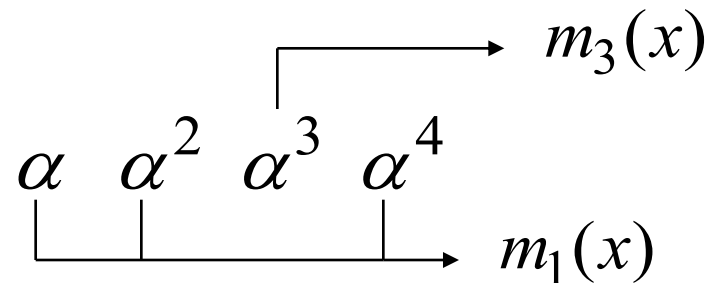
$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \vdots & & & & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{2t(n-1)} \end{bmatrix}_{2t \times n}$$

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

Any $2t$ columns are linearly independent

$$\therefore d > 2t$$

- Example:



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

Therefore, for $d = 5$, only the rows

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

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

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

Theorem 8.1 – The 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 $GF(q^m)$, $n \mid q^m - 1$. If $g(x)$ is the monic polynomial of smallest degree such that

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

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

$$g(x) = \text{LCM}\{m_b(x), m_{b+1}(x), m_{b+\delta-2}(x)\}$$

- The most commonly encountered BCH codes are the
 $n = q^m - 1$ **primitive** (α is a primitive element)

$$b = 1 \quad \text{**narrow-sense**}$$

BCH codes

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

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

product of t minimal polynomials of degree m or less

- d is called the **designed distance**
- For $q = 2$, every second row in the \mathbf{H} matrix can be deleted as α^2 has the same minimal polynomial as α
- Binary examples:

$d = 3$ $(2^m-1, 2^m-1-m, 3)$ Cyclic Hamming code

$$g(x) = m_1(x)$$

$d = 5$ $(2^m-1, 2^m-1-2m, 5)$ BCH code

$$g(x) = m_1(x)m_3(x)$$

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 $\text{GF}(q^m)$ where m is minimal
 - 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: BCH Codes of Length 31

- Let α be a root of x^5+x^2+1 $n = 2^5-1 = 31$
- Determine the cyclotomic cosets modulo 31

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	$\alpha, \alpha^2, \alpha^3, \dots, \alpha^6$	$m_1(x)m_3(x)m_5(x)$	(31,16,7)
4	$\alpha, \alpha^2, \alpha^3, \dots, \alpha^8$	$m_1(x)m_3(x)m_5(x)m_7(x)$	(31,11,11)

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

BCH Codes with $b = 0$

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

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

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

$$\mathbf{G} = \begin{bmatrix} 1011100 \\ 0101110 \\ 0010111 \end{bmatrix}$$

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

$$\mathbf{H} = \begin{bmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{bmatrix}$$

Minimal Polynomials GF(64)

$\{1,2,4,8,16,32\}$	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	$m_7(x)$
$\{11,22,44,25,50,37\}$	$x^6+x^5+x^3+x+1$	$m_{11}(x)$
$\{13,26,52,41,19,38\}$	$x^6+x^4+x^3+x+1$	$m_{13}(x)$
$\{15,30,60,57,51,39\}$	$x^6+x^5+x^4+x^2+1$	$m_{15}(x)$
$\{21,42\}$	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	$m_{31}(x)$

BCH Codes of Length 63

$(63,57,3)$	$(63,51,5)$	$(63,45,7)$
$(63,39,9)$	$(63,36,11)$	$(63,30,13)$
$(63,24,15)$	$(63,18,21)$	$(63,16,23)$
$(64,10,27)$	$(63,7,31)$	

Non-primitive BCH Codes

- Example $n = 21, q = 2, m = ?$
 $n \mid 2^m - 1$ $m = 6$ (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 $\beta, \beta^2, \beta^3, \beta^4 \rightarrow \alpha^3, \alpha^6, \alpha^9, \alpha^{12}$
$$g(x) = (x^6 + x^4 + x^2 + x + 1)(x^3 + x^2 + 1)$$
$$= x^9 + x^8 + x^7 + x^5 + x^4 + x + 1$$

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

- There are many cases where the actual minimum distance is greater than the designed distance
- Example: construct a BCH with $n = 23$
 $23 \mid 2^{11}-1 \rightarrow \text{GF}(2^{11}) \quad 2^{11}-1 = 23 \times 89$
- Let α be a primitive element in $\text{GF}(2^{11})$
- $\beta = \alpha^{89}$ so that $\beta^{23} = \alpha^{89 \times 23} = 1$
 - $t = 1$: required roots are β, β^2
 - adding the conjugates, the roots are:
 $\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32} = \beta^9, \beta^{18}, \beta^{13}, \beta^3, \beta^6, \beta^{12}$
- $g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$
- designed distance is 5: code parameters are $(23, 12, 7)$