Generator and parity check matrices of cyclic codes:

The generator polynomial of an (n,k) cyclic code is given by

$$g(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_2x^2 + g_1x + g_0$$

The generator matrix is given by

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

Ex: (7,4) Hamming code has generator polynomial

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

Its generator matrix is

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

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

Exercise: For the previous example put G into systematic form

answer
$$G=\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Parity check matrix of an (n,k) cyclic code is given by

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

The parity check matrix of the (n,k) cyclic code is obtained from

$$H=\begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{k-2} & h_k & 0 & \cdots & 0 \\ 0 & h_0 & h_1 & \cdots & \cdots & h_{k-1} & h_k & \cdots & 0 \\ \vdots & & & & & & & & \\ 0 & \cdots & \cdots & h_0 & h_1 & \cdots & \cdots & h_k & 0 \\ 0 & \cdots & \cdots & 0 & h_0 & h_1 & \cdots & h_{k-1} & h_k \end{bmatrix}$$

↓ Parity check matrix of an (n,k) cyclic code.

(31)

Ex: (7,4) Hamming code

has generator polynomial $g(x) = x^3 + x + 1$

and parity-check polynomial

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

$h_4 = 1$ $h_3 = 0$ $h_2 = 1$ $h_1 = 1$ $h_0 = 0$

The parity check matrix is

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

which gives

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

Exercise

Given that

$$x^{15} + 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

a) Determine the number of cyclic codes with blocklength 15

b) The number of (15,11) cyclic codes

c) The generator and parity check poly. for the (15,7) cyclic codes

d) For part c, determine generator matrix and parity check matrix of the cyclic codes.

e) Determine minimum distance of cyclic codes in part d, obtain syndrome tables

Exercise 2

$g(x) = x^8 + x^7 + x^6 + x^4 + x^2 + 1$ be the generator polynomial of a cyclic code.

Let $m(x) = 1 + x + x^3 + x^5 + x^7 + x^{12} + x^{16} + x^{21}$ be the message polynomial

Determine codeword polynomial $c(x)$ in systematic & non-systematic form.

Exercise 3 The following polynomials are code polynomials from binary cyclic codes. Determine the highest-degree generator $g(x)$ for each code

a) $c(x) = 1 + x^4 + x^5$

b) $c(x) = 1 + x^8$

c) $c(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + x^{10}$

Galois Fields

Consider the roots of $x^2 - 4 = 0$

roots are $-2, +2$ which are in real number fields.

$1, 2, -2, +2 \in R$

Now consider the equation

$$x^2 + 4 = 0$$

Roots cannot be found in real numbers field. We extend the real numbers field and obtain complex number fields.

$$x^2 + 4 = 0 \longrightarrow x_{1,2} = \pm 2j \in \mathbb{C}$$

$\mathbb{C}$ ↓ complex field

real field $\xrightarrow{\text{extension}}$ complex field

real field ↓ base field

complex field ↓ extended field.

real field & complex field are infinite fields. Fields can also contain finite number of elements.

Ex: Binary field $F_2 = \{0, 1\}$ → only has two elements

such fields are called finite fields.

We also know that if $a+jb$ is a root an equation then $a-jb$ is also another root

$a-jb$ is called conjugate of $a+jb$

The Galois Field

Consider the equation and binary field $F_2=\{0,1\}$

$x^2+1=0$ → This equation has a solution in binary field $F_2=\{0,1\}$

Solution is 1

i.e, $1^2+1=0$ $\quad x^2+1=0 \rightarrow x=+1$

solution

Now consider $x^2+x+1=0$ and search its root in $F_2=\{0,1\}$

$0^2+0+1=0$ ✗ neither 0 nor 1 is a solution

$1^2+1+1=0$ ✗

we extend $F_2=\{0,1\}$ to a new finite field and look for the solutions inside the new field.

Assume that extended field is G and

$\alpha \in G$ is a root of $x^3+x+1=0$

i.e, $\alpha \in G$ and $\alpha^3+\alpha+1=0$ ✓

What about other elements of G

$\alpha^3+\alpha+1=0 \qquad \alpha \in G$

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

The other elements of G are the all the other polynomials with degree less than or equal to 2

Other elements of G are

$$0, 1, \alpha, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1, \alpha^2$$

i.e, $G=\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

↓

we have 8 elements in this field.

We can really show that G is a field with 8 elements and satisfy the properties of a field

i.e,

$\oplus$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0								
1								
α								
α^2								
α^2+1								
$\alpha^2+\alpha$								
$\alpha^2+\alpha+1$								

$\odot$	0	1	α	...	$\alpha^2+\alpha+1$
0					
1					
α					
⋮					
$\alpha^2+\alpha+1$					

↓ fill the tables.

96

Consider G again

$$G = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

where α is a root of $x^3+x+1=0$

i.e, $\alpha^3+\alpha+1=0 \longrightarrow \alpha^3 = \alpha+1$

From G we see that all the elements of G can be generated using powers of α and using the equality $\alpha^3=\alpha+1$.

i.e, $G = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

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

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

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

We see that G contains 8 elements $8 = 2^3$

polynomial degree is 3
(x^3+x+1)

Hence G is usually called $GF(2^3)$ → Galois Field with 8 elements generated by a polynomial of degree 3 and the base field is the binary field with 2 elements

Now we ask the questions

if $p(x)$ has a polynomial of degree n then using $p(\alpha)=0$ and taking successive powers of α can we generate an extended finite field with 2^n elements.

The answer is: If $p(x)$ is a primitive polynomial then the answer is yes. If $p(x)$ is not primitive but irreducible polynomial then the power of α (power of root) may not generate all the elements of extended field. Let's see the definition of irreducible and primitive polynomials.

Irreducible Polynomials:

A polynomial $p(x)$ with degree r is irreducible if $p(x)$ divides x^n+1 where $n=2^r-1$ and and irreducible polynomial cannot be factorized

Ex: $x^3+x+1 \rightarrow$ cannot be factorized

x^3+x+1 divides x^7+1 $\quad 7=2^3-1$

Primitive Polynomial:

A polynomial $p(x)$ with degree r is primitive if $p(x)$ divides polynomial x^n+1 where: $n=2^r-1$ and $p(x)$ does not divide polynomials (x^n+1) with degree less than $n=2^r-1$.

Remark: An irreducible polynomial $p(x)$ with degree r divides x^n+1 where $n=2^r-1$ and $p(x)$ may divide other polynomials x^n+1 with degree less than 2^r-1.

Ex: Show that x^3+x+1 is primitive polynomial

If x^3+x+1 is primitive then

a) x^3+x+1 divides x^7+1

b) // doesn't divide x^6+1

c) // // // x^5+1

d) // doesn't divide x^4+1

If we check all a, b, c, d we see that all are satisfied and x^3+x+1 is a primitive polynomial

Ex° Show that $p(x) = x^4+x^3+x^2+x+1$ is an irreducible polynomial but it is not a primitive polynomial.

S/n° If $p(x)$ is irreducible then $p(x)$ divides x^n+1 where $n=2^r-1$ $r \to$ degree of $p(x)$

$x^4+x^3+x^2+x+1$ divides $x^{15}+1$

and we can show that

$x^4+x^3+x^2+x+1$ also divides x^5+1

So $x^4+x^3+x^2+x+1$ is an irreducible polynomial but it is not a primitive polynomial

Remark° Every primitive polynomial is an irreducible polynomial, but, every irreducible polynomial is not a primitive polynomial.

Lemma:

$p(x)$ is a polynomial with degree r

is primitive if $n = 2^r - 1$ is a prime number

However, if $n = 2^r - 1$ is not a prime number $p(x)$ may or may not be a primitive polynomial.

Ex:

$p(x) = x^3 + x + 1 \rightarrow n = 2^3 - 1 = 7 \rightarrow$ prime number

$p(x) \rightarrow$ primitive polynomial

$p(x) = x^4 + x + 1 \rightarrow n = 2^4 - 1$

$= 15 \rightarrow$ not a prime number

However $p(x)$ is still primitive

$p(x) = x^4 + x^3 + x^2 + x + 1 \rightarrow n = 2^4 - 1$

$= 15 \rightarrow$ not a prime number

$p(x)$ is not a primitive polynomial

Exercise:

Show that $p(x) = x^4 + x + 1$

is a primitive polynomial.

Now. we return to the Galois fields:

if degree of $p(x)$ is r and $p(x)$ is a primitive polynomial then roots of $p(x)$ can be used to generate all the other field elements, $p(x)$ with degree r can be used to generate an extended field with 2^r elements.

Base field (Binary field) 2 elements $\xrightarrow{\text{Extend using } p(x)}$ $GF(2^r)$ ≙ Galois finite field with 2^r elements.

Ex: $p(x) = x^4 + x + 1$ is a primitive polynomial construct $GF(2^4)$ using $p(x)$.

Sln: $p(x) = 0 \rightarrow$ let $\alpha \in GF(2^4)$

and $p(\alpha) = 0 \longrightarrow \alpha^4 + \alpha + 1 = 0 \rightarrow \boxed{\alpha^4 = \alpha + 1}$

then successive power of α generate all the field elements

i.e, $GF(2^4) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$

102

$\alpha^4 = \alpha + 1$

$0 \longrightarrow 0$

$1 \longrightarrow 1$

$\alpha \longrightarrow \alpha$

$\alpha^2 \longrightarrow \alpha^2$

$\alpha^3 \longrightarrow \alpha^3$

$\alpha^4 \longrightarrow \alpha + 1$

$\alpha^5 \longrightarrow \alpha\alpha^4 = \alpha(\alpha+1) \longrightarrow \alpha^2 + \alpha$

$\alpha^6 \longrightarrow \alpha\alpha^5 = \alpha(\alpha^2+\alpha) \longrightarrow \alpha^3 + \alpha^2$

$\alpha^7 \longrightarrow \alpha\alpha^6 = \alpha(\alpha^3+\alpha^2) \longrightarrow \alpha^4 + \alpha^3 \longrightarrow \alpha+1+\alpha^3$

$\alpha^8 \longrightarrow \alpha\alpha^7 = \alpha(\alpha^3+\alpha+1) \longrightarrow \alpha^4+\alpha^2+\alpha \longrightarrow \alpha+1+\alpha^2+\alpha$

$\alpha^9 \longrightarrow \alpha\alpha^8 = \alpha(\alpha^2+1) \longrightarrow \alpha^3+\alpha$

$\alpha^{10} \longrightarrow \alpha\alpha^9 = \alpha(\alpha^3+\alpha) \longrightarrow \alpha^4+\alpha^2 \longrightarrow \alpha+1+\alpha^2$

$\alpha^{11} \longrightarrow \alpha\alpha^{10} = \alpha(\alpha^2+\alpha+1) \longrightarrow \alpha^3+\alpha^2+\alpha$

$\alpha^{12} \longrightarrow \alpha\alpha^{11} = \alpha(\alpha^3+\alpha^2+\alpha) \longrightarrow \alpha^4+\alpha^3+\alpha^2 \longrightarrow \alpha+1+\alpha^3+\alpha^2$

$\alpha^{13} \longrightarrow \alpha\alpha^{12} = \alpha(\alpha^3+\alpha^2+\alpha+1) \longrightarrow \alpha^4+\alpha^3+\alpha^2+\alpha \longrightarrow \alpha+1+\alpha^3+\alpha^2+\alpha$

$\longrightarrow \alpha^3+\alpha^2+1$

$\alpha^{14} \longrightarrow \alpha\alpha^{13} = \alpha(\alpha^3+\alpha^2+1) \longrightarrow \alpha^4+\alpha^3+\alpha$

$\longrightarrow \alpha+1+\alpha^3+\alpha$

$\longrightarrow \alpha^3+1$

Hence:

$0 \longrightarrow 0$

$1 \longrightarrow 1$

$\alpha \longrightarrow \alpha$

$\alpha^2 \longrightarrow \alpha^2$

$\alpha^3 \longrightarrow \alpha^3$

$\alpha^4 \longrightarrow \alpha+1$

$\alpha^5 \longrightarrow \alpha^2+\alpha$

$\alpha^6 \longrightarrow \alpha^3+\alpha^2$

$\alpha^7 \longrightarrow \alpha^3+\alpha+1$

$\alpha^8 \longrightarrow \alpha^2+1$

$\alpha^9 \longrightarrow \alpha^3+\alpha$

$\alpha^{10} \longrightarrow \alpha^2+\alpha+1$

$\alpha^{11} \longrightarrow \alpha^3+\alpha^2+\alpha$

$\alpha^{12} \longrightarrow \alpha^3+\alpha^2+\alpha+1$

$\alpha^{13} \longrightarrow \alpha^3+\alpha^2+1$

$\alpha^{14} \longrightarrow \alpha^3+1$

Thus

$GF(2^4) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha+1, \alpha^2+\alpha, \alpha^3+\alpha^2, \alpha^3+\alpha+1, \alpha^2+1, \alpha^3+\alpha, \alpha^2+\alpha+1,$
$\alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1, \alpha^3+\alpha^2+1, \alpha^3+1\}$

Exercise:

$p(x) = x^5 + x^2 + 1$ is a primitive polynomial. Using $p(x)$ generate all the field elements of $GF(2^5)$.

i.e, construct the extended field $GF(2^5)$ from base field $F_2 = \{0, 1\}$, i.e, binary field

Example:

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

is an irreducible polynomial but it is not a primitive polynomial.

Using $p(x)$ construct $GF(2^4)$

Sln: Assume that $\alpha \in FG(2^4)$ and α is a root of $p(x)$ i.e, $p(\alpha) = 0$

then we have $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$

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

If $p(x)$ was primitive and $p(\alpha)=0$ then successive powers of α generate field elements. Let's do it for irreducible $p(x)$

$$\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$$

α is a root of $p(x)$, i.e, $p(\alpha)=0$

$0 \longrightarrow 0$

$1 \longrightarrow 1$

$\alpha \longrightarrow \alpha$

$\alpha^2 \longrightarrow \alpha^2$

$\alpha^3 \longrightarrow \alpha^3$

$\alpha^4 \longrightarrow \alpha^3+\alpha^2+\alpha+1$

$\alpha^5 \longrightarrow \alpha\alpha^4 = (\alpha)(\alpha^3+\alpha^2+\alpha+1)$

$= \alpha^4+\alpha^3+\alpha^2+\alpha$

$= \alpha^3+\alpha^2+\alpha+1 + \alpha^3+\alpha^2+\alpha$

$= 1$

$\alpha^6 \longrightarrow \alpha\alpha^5 = \alpha \longrightarrow$ but this is already generated, field elements must be different from each other

Hence successive power of α which is a root of $p(x)$ (irreducible polynomial) cannot generate all the other field elements.

However there can be a β element of $GF(2^4)$ which is not a root of $p(x)$ may generate all the field elements

$\alpha \rightarrow$ root of $p(x) \longrightarrow p(\alpha)=0$

$\alpha^4=\alpha^3+\alpha^2+\alpha+1$

Let $\beta=\alpha+1 \rightarrow$ not a root of $p(x)$

It can be shown that successive powers of β can generate all the other field elements.

$\alpha^4=\alpha^3+\alpha^2+\alpha+1$ $\quad$ $\beta=\alpha+1$

$0 \longrightarrow 0$

$1 \longrightarrow 1$

$\beta^1 \longrightarrow \alpha+1$

$\beta^2 \longrightarrow \alpha^2+1$

$\beta^3 \longrightarrow \alpha^3+\alpha^2+\alpha+1$

$\beta^4 \longrightarrow \alpha^3+\alpha^2+\alpha$

$\beta^5 \longrightarrow \alpha^3+\alpha^2+1$

$\beta^6 \longrightarrow \alpha^3$

$\beta^7 \longrightarrow \alpha^2+\alpha+1$

$\beta^8 \longrightarrow \alpha^3+1$

$\beta^9 \longrightarrow \alpha^2$

$\beta^{10} \longrightarrow \alpha^3+\alpha^2$

$\beta^{11} \longrightarrow \alpha^3+\alpha+1$

$\beta^{12} \longrightarrow \alpha$

$\beta^{13} \longrightarrow \alpha^2+\alpha$

$\beta^{14} \longrightarrow \alpha^3+\alpha$

$\beta^{15} \longrightarrow 1$

take one of them.

Conjugate classes

If $1+j$ is a root of a polynomial then $1-j$ is another root.

$1+j$ & $1-j$ is a conjugate class

A similar concept holds for the elements of a finite field

Given that β is a field element in $GF(2^r)$ then the conjugates of β are

$$\beta, \beta^2, \beta^4, \beta^8, \ldots \beta^{2^m-1}$$

where m is the smallest integer such that $\beta^{2m} = \beta$

Ex: $GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ and $\alpha^7 = 1$

Determine the conjugates of α^3 in $GF(2^3)$

Sln:

let $\beta = \alpha^3$

then $\beta^2 = \alpha^6$

$\beta^4 = \alpha^{12}$

$= \alpha^7 \cdot \alpha^5$

$= \alpha^5$

$\beta^8 = \alpha^{24}$

$= \alpha^{21} \cdot \alpha^3$

$= \alpha^3$

So conjugates of α^3 are

$\alpha^3, \alpha^5, \alpha^6$

Ex° Determine all the conjugates of α^3 in GF(24)

S/n° In GF(24) we have $\alpha^{15}=1$ where α is a root of a primitive polynomial.

Conjugates of α^3 are

$(\alpha^3)^2 \longrightarrow \alpha^6$

$(\alpha^3)^4 \longrightarrow \alpha^{12}$

$(\alpha^3)^8 \longrightarrow \alpha^{24} = \alpha^{15}\alpha^9 = \alpha^9$ ($\alpha^{15} \to 1$)

$(\alpha^3)^{16} \longrightarrow \alpha^{48} = \alpha^{45}\alpha^3 = \alpha^3$ ($\alpha^{45} \to 1$) → stop here

$(\alpha^3)^{32} \longrightarrow \alpha^{96} = \alpha^{80}\cdot\alpha^6 = (\alpha^{15})^5\alpha^6 = \alpha^6$ ($\alpha^{15} \to 1$) → repeated no need to continue.

Hence the conjugate class of α^3 is $\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$

Defn° Given a GF(2^m) and $\beta \in$ GF(2^m) the order of β is an integer n such that $\beta^n = 1$

Ex: Let $p(x)$ be a primitive polynomial and α is a root of $p(x)$. The degree of $p(x)$ is 4. The polynomial $p(x)$ can be used to generate

$GF(2^4) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \ldots \alpha^{14}\}$

$\alpha^{15} = 1$

The field elements and their orders may be tabulated as below given.

Elements:	order
$\alpha, \alpha^2, \alpha^4, \alpha^8$	15
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	5
α^5, α^{10}	3
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	15

Remark: In a conjugate class, all the elements have the same order

Remark: If an element β of $GF(2^m)$ is primitive then its conjugates are also primitive.

Lemma: In $GF(2^m)$ let $\beta \in GF(2^m)$
If order of β is k, i.e, $\beta^k = 1$ then k divides $2^m - 1$

Defn: In $GF(2^m)$ primitive elements have order 2^m-1 and using any primitive element all other field elements can be generated.

Ex: Given $GF(2^6)$ what can be the order of elements

Sln:
$$2^6-1 = 64-1$$
$$= 63$$

$$63 = 9 \cdot 7$$
$$= 3 \cdot 3 \cdot 7$$

Hence orders can be 3, 9, 7, 21, 63 (all divide 63)

Minimal Polynomials

Consider the roots of a polynomial

Lets say that roots are $1+j$ $1-j$
$2+j$ $2-j$

then we can form the polynomial as $(x-(1+j))(x-(1-j))(x-(2+j))(x-(2-j))$

$\Downarrow$ $\Downarrow$

$(x^2-x(1-j)-x(1+j)+2)$ $(x^2-x(2-j)-x(2+j)+5)$

$\Downarrow$ $\Downarrow$

(x^2-2x+2) (x^2-4x+5)

$(x-(1+j))(x-(1-j))(x-(2+j))(x-(2-j))$

$\Downarrow$ $\Downarrow$

(x^2-2x+2) (x^2-4x+5)

These are called minimal polynomials

x^2-2x+2 → is the minimal polynomial of $1+j$ or $1-j$

x^2-4x+5 → is the minimal polynomial of $2-j$ or $2+j$

In a similar manner, if conjugate classes of a field is given we can find a minimal polynomial for each conjugate class

Ex:- in $GF(2^3)$ find conjugates of α and find minimal polynomial for the found conjugate class

Sln:- Conjugates of α are $\alpha^7=1$

α^2

α^4

$\alpha^8=\alpha^7\alpha=\alpha$

Hence conjugate class is $\{\alpha, \alpha^2, \alpha^4\}$

(111)

The minimal polynomial associated with the conjugate class is

$$m(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$$

If we further simplify the expression

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4) = (x^2-\alpha^2x-\alpha x+\alpha^3)(x-\alpha^4)$$

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4) = (x^2-\alpha^2x-\alpha x+\alpha^3)(x-\alpha^4)$$

$$= (x^2-(\alpha^2+\alpha)x+\alpha^3)(x-\alpha^4)$$

Assume that we use primitive polynomial $p(x)=x^3+x+1$ to generate $GF(2^3)$ then $\alpha^3=\alpha+1$

$$= (x^2-(\alpha^2+\alpha)x+(\alpha+1))(x-\alpha\alpha^3)$$

($\alpha^3 \to \alpha+1$)

$$= (x^2-(\alpha^2+\alpha)x+(\alpha+1))(x-\alpha(\alpha+1))$$

$$= x^3-\alpha(\alpha+1)x^2-\alpha(\alpha+1)x^2+\alpha^2(\alpha+1)^2x+(\alpha+1)x - \alpha(\alpha+1)^2$$

$$= x^3+\alpha^2(\alpha+1)^2x+(\alpha+1)x-\alpha(\alpha+1)^2$$

$$= x^3+(\alpha^2(\alpha^2+1)+\alpha+1)x-\alpha(\alpha^2+1)$$

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

($\alpha\alpha^3 \to \alpha+1$)

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

$\alpha\alpha^3 \to \alpha + 1$

$$= x^3 + (\alpha^2 + \alpha + \alpha^2 + \alpha + 1)x - (\alpha^3 + \alpha)$$

$\alpha^3 \to \alpha + 1$

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

$$= x^3 + x - 1$$

$$= x^3 + x + 1$$

Hence the minimal polynomial of the conjugate class $\alpha, \alpha^2, \alpha^4$ is $m(x) = x^3 + x + 1$

Notice that no α terms appear in $m(x)$

As in complex conjugate case even though roots are complex the polynomial coefficients are all real.

Similarly even though the roots are in extended field, the polynomial coefficients are in base field.

Exercise: $p(x) = x^3 + x + 1$ $GF(2^3)$

Show that the minimal polynomial of $\{\alpha^3, \alpha^5, \alpha^6\}$ is $m(x) = x^3 + x^2 + 1$

To summarize:

$GF(2^3)$ conjugate classes and their minimal polynomials are shown in the table below

Conjugate Classes in $GF(2^3)$	Minimal Polynomials
0	x
1	$x+1$
$\alpha, \alpha^2, \alpha^4$	x^3+x+1
$\alpha^3, \alpha^5, \alpha^6$	x^3+x^2+1

Now consider the product of the minimal polynomials

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

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

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

$$= x^7 + x^6 + x^4 + x^6 + x^5 + x^3 + x^5 + x^4 + x^2 + x^2 + x^2 + 1$$

$$= x^7 + 1$$

We below show the conjugate classes and minimal polynomials for $GF(2^4)$

Conjugate Classes:	Minimal Polynomials:
0	X
1	$X+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	X^4+X+1
α^5, α^{10}	X^2+X+1
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4+X^3+X^2+X+1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	X^4+X^3+1

Lets verify that the minimal polynomial of $\{\alpha^5, \alpha^{10}\}$ is X^2+X+1

$$(X-\alpha^5)(X-\alpha^{10}) = X^2 - \alpha^{10}X - \alpha^5 X + \underbrace{\alpha^{15}}_{=1}$$

$$= X^2 - \underbrace{(\alpha^{10}+\alpha^5)}_{=1} X + 1$$

$p(X) = X^4 + X + 1$ is used to generate $GF(2^4)$

$p(\alpha) = 0 \rightarrow \alpha^4 = \alpha + 1$

Notations: if α^i belongs to a conjugate class the minimal polynomial of the conjugate class is denoted by $m_i(X)$

Since all the elements in the conjugate class have the same minimal polynomial we can write

$$m_i(x) = m_{2i}(x) = m_{4i}(x) = m_{8i}(x) \cdots$$

Note: Conjugates of α^i are $\alpha^{2i}, \alpha^{4i}, \alpha^{8i}, \alpha^{16i}, \alpha^{32i}, \ldots$

Ex: In GF(2³) the conjugate class is given as $\{\alpha, \alpha^2, \alpha^4\}$

and the minimal polynomial of this class is $m(x) = x^3 + x + 1$

This can also be written as

$m_1(x) = x^3 + x + 1$ → minimal poly. of α

$m_2(x) = x^3 + x + 1$ → // // // α^2

$m_4(x) = x^3 + x + 1$ → // // // α^4

$$m_1(x) = m_2(x) = m_4(x)$$

Property: In GF(2^m)

$$(x_1 + x_2 + \cdots x_n)^2 = x_1^2 + x_2^2 + \cdots x_n^2$$

OR more generally

$$(x_1 + x_2 + \cdots + x_n)^{2^i} = (x_1^{2^i} + \cdots x_n^{2^i})$$

116

Ex° $(X_1+X_2)^2 = X_1^2 + X_1X_2 + X_2X_1 + X_2^2$

$= X_1^2 + X_2^2$

Ex° $(X_1+X_2)^6 = (X_1+X_2)^4 (X_1+X_2)^2$

$= (X_1^4 + X_2^4)(X_1^2 + X_2^2)$

$= X_1^6 + X_2^2 X_1^4 + X_2^4 X_1^2 + X_2^6$

Ex° Exprimer $(X+\alpha^4)^2$ in $GF(2^3)$

Sln° $(X+\alpha^4)^2 = X^2 + (\alpha^4)^2$

$= X^2 + \alpha^8$ in $GF(2^3)$ $\alpha^7 = 1$

$= X^2 + \alpha \alpha^7 = 1$

$= X^2 + \alpha$

Ex° in $GF(2^4)$ $\alpha^{15} = 1$

$(X+\alpha^7)^8 = X^8 + \alpha^{56}$

$= X^8 + \alpha^{45} \alpha^{11}$

$= X^8 + \alpha^{11}$

Exercises

1) Determine whether the polynomials

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

$p_2(x) = x^2 + x + 1$

$p_3(x) = x^3 + x^2 + 1$

over GF(2) are irreducible and primitive

2) Using $p(x) = x^2 + x + 1$ construct $GF(2^2)$

a) find all the conjugate classes

b) and find all the minimal polynomials

3) $p(x)$ a primitive polynomial used to construct $GF(2^4)$ $p(\alpha) = 0$

Determine such a $p(x)$

Find the roots of $x^3 + \alpha^8 x^2 + \alpha^{12} x + \alpha = 0$

defined over $GF(2^4)$

4) in $GF(2^4)$

find $\sqrt{\alpha^5}$

in $GF(2^3)$ find $\sqrt{\alpha^5}$

Example: In $GF(2^5)$ find $\sqrt{\alpha^3}$

Sln: In $GF(2^5)$ $\alpha^{15} = 1$

$$\sqrt{\alpha^3} = \sqrt{\alpha^3 \alpha^{15}}$$
$$= \sqrt{\alpha^{18}}$$
$$= \alpha^9$$

Exercise: Solve the linear equations

$$\alpha^{10}x + \alpha^4 y + \alpha z = \alpha^9$$
$$\alpha^5 x + \alpha^{12} y + z = \alpha^4$$
$$\alpha^2 x + \alpha^4 y + \alpha^7 z = \alpha^7$$

defined over $GF(2^3)$ use $p(x) = x^3 + x + 1$ as your primitive polynomial.

Example: Prove that $p(x) = x^2 + x + 2$

a) is irreducible in $GF(3)$

b) construct the field $GF(3^2)$ using the primitive polynomial $p(x) = x^2 + x + 2$