V.J.T.I

T.Y.B.Tech.(ExTC)

Sub: Digital Communication System

Sem-V

Course Instructor

Dr. D. P. Rathod

PhD(Technology)Electronics Engg.

Dept. of Electronics Engineering

dprathod@el.vjti.ac.in

Mob-9819003515

Research Area Includes

- Error correcting Codes/coding theory
- Wireless Communication
- FOC / Microwave
- Micro Strip Antennas
- IOT
- Wireless Sensor Networks
- Mobile/Vehicular Adhoc Networks
- ML
- Embeded Systems
- Signal processing

Error Correcting Codes

- **Block diagram of modern digital communication system**
- **Error correcting codes/coding theory/ Channel coding**
- **Hamming code(n, k)/Cyclic code(n,k)**
- **Code rate and valid code set**
- **Properties of matrix**
- **Modern linear abstract Algebra-**
- **Groups**
- **Fields**
- **Vector spaces**

Code rate and code word set

- Code rate $r = k/n$

- Valid code word set C

- For (n, k) linear block code,
  2^k , are the set of valid code word of length n bits

- These 2^k Code words are obtained by taking linear combination of rows of a G matrix and mod-2 operation

- Rows of G matrix should be linearly independent

Properties of Matrices

- Design of (n, k) code requires generator matrix G or generator polynomial for encoding at transmitter side

- Parity check Matrix H or parity check polynomial at receiver side in order to decode/ recover the original data

- The required matrices and polynomials should have important properties as follows-

Matrix properties

- The rows and columns of both matrices should be linearly independent
- No two or more number of columns or rows should be equal
- Both Matrices should be in systematic form
- No rows or columns should have all elements zero’s

Modern Linear Abstract Algebra

- Much of this work for **ECC** is mathematics in nature, requires an extensive background in **modern algebra theory** to understand.
- Brief Introduction of Modern linear abstract algebra
  - Group
  - Fields
  - Vector Spaces
  - Irreducible polynomial *P(X) of degree m*
  - *Primitive Polynomial P(X) of degree m*
  - *Extension of Field GF(* 2^m *)*
  - *factorization of* $X^n + 1$ *over GF(2)*

Modern Linear Abstract Algebra

- Cyclic codes are constructed using polynomial form hence easy to implement using simple shift registers and logic gates, switches etc.

- In cyclic codes generator polynomial of degree (n-k) is required to construct a code **(channel Encoding)**

- The generator polynomial is a factor of $X^n + 1$ over GF(2)={0,1}

- Where, $n=2^m -1$ and m is degree of irreducible polynomial

Modern Linear Abstract Algebra

Systematic structure of G and H

Generator matrix **'G'** is

$$G_{k \times n} = [I_k \;\; P_{k \times (n-k)}]$$

where,

G is a generator matrix of size k×n

I is a identity matrix of size k×k

P is a parity bit matrix of size k×(n-k)

The **'G' matrix** is derived from **Parity Check matrix 'H',**

where ,

$$H_{(n-k) \times n} = [P^T \;\; I_{n-k}]$$

Relation between matrix G and H is such that

$$H.G^T = 0$$

Modern Linear Abstract Algebra

- As relation between matrix G and H is such that

$$\mathbf{H.G^T = 0} \qquad \text{.......1}$$

- All code words *C* are generated by using G matrix, hence G can be replaced by *C in eq.1*
- $H.C^T = 0$ *mod-2 operation*
- *Let* $c = r$
- $\mathbf{r.H^T = 0}$ or $\mathbf{H.r^T = 0}$ mod-2 operation,
- This is the condition to check validity of received code words

Hamming (n,k) code

- $C = m.G$ mod-2 (Encoding)
- $R.H^T = 0$ mod-2 (decoding)

Modern Linear Abstract Algebra

- **Groups G**
  - Let G be a set of elements.
  - A *binary operation* * on G is *rule* that assigns to each pair of elements **a** and **b** , third element c = a* b in G.
  - Then we say that **G is *closed*** under *.
  - Hence, the set of integer is *closed* under real addition.

Modern Linear Abstract Algebra

- ***Groups:***
  - A binary operation * on G is said to be *associative* if, for any a ,b, & c in G.

    $$a \; * (b * c) = (a * b) * c.$$

  - G contains an element e such that for any a in G, $a \; * e = e * a = a$ This element e is called an identity element.
  - For any element a in G there exist another element a' in G such that $a * a' = a' * a = e$. The element a' is called an inverse of a(a is also an inverse of a').
  - A group G is said to be commutative if its binary operation * also satisfies the following conditions :
  - For any a & b in G,

    $$a \; * b = b * a.$$

Modern Linear Abstract Algebra

- ***Groups :***
  - ***Example***
  - The set of all integer is a commutative group under real addition.
  - In this case, the integer 0 is the identity element, & the integer –i is the inverse of integer i.
  - The set of all rational numbers excluding zero is a commutative group under real multiplication.
  - The integer 1 is the identity element with respect to real multiplication, & the rational number ${}^{b}/_{a}$ is the multiplicative inverse of ${}^{a}/_{b}$.
  - Groups with finite numbers of elements do exist, as we shall in the next example.
  - The number of elements in a group is called as ***order of the group.***
  - A group of finite order is called a ***finite group***.

Modern Linear Abstract Algebra

➢ Group:

➢ Example :

Consider the set of two integers $G = \{0,1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows

➢ **Solution**

$0 \oplus 0 = 0.$ $0 \oplus 1 = 1$ $1 \oplus 0 = 1$ $1 \oplus 1 = 0$

This binary operation is called *modulo-2* addition. The set $G = \{0,1\}$ is a group under *modulo-2* addition. It follows from the definition of *modulo-2* addition $\oplus$ that G is closed under $\oplus$, & $\oplus$ is commutative. The inverse of 0 is itself, and the inverse of 1 is also itself, thus G together with $\oplus$ is a commutative group.

➢ For any positive integer m, it is possible to construct a group of order m under a binary operation that is very similar to real addition.

Modern Linear Abstract Algebra

➢ ***Fields:***

- Let F be a set of elements on which two binary operations called addition "+" & multiplication "."are defined.
- The set F together with the two binary operations "+" & "." ,Is a field if the following conditions are satisfied:

i. F is commutative group under addition +.

ii. The identity element with respect to addition is called the *zero elements or*

iii. The *additive identity* of F & is denoted by 0.

iv. The set of nonzero elements in F is a commutative group under multiplicative identity of F and is denoted by 1.

v. Multiplication is distributive over addition; that is, for any three elements a, b, & c in F

$$a.(b+c) = a.b + a.c$$

Modern Linear Abstract Algebra

- ***Fields:***
  - Hence, a field consist of at least two elements, the additive and multiplicative identity.
  - The number of elements in field is called as **orde**r of the field.
  - A field with a finite number if elements is called a **finite** field.

Modern Linear Abstract Algebra

- ***Fields***
- In a field the additive inverse of an element a is denoted by $-a$, and the multiplicative inverse of a is denoted by a^{-1}.
- For Example:
- $GF(2) = \{0, 1\}$ is the smallest field of Galois Field of 2 element.

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :*** Let *V* be a set of elements on which a binary operation called addition, +, is defined.
- Let *F* be a field. GF(2)={0,1}
- A multiplication operation by **"."**, between the elements in *F* and elements in *V* is also defined.
- The set *V* is called a *vector space* over the field *F* if it satisfies the following conditions:
  - *V* is Commutative under addition. **(u+v = v+u)**
  - For any element a in *F* and any element **v** in *V*, a.**v** is an element in *V*.

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
  - Let n =5. the vector space V_5 of all 5-tuples over GF(2) consist of the following set of 32 vectors which are distinct :

(00000)	(00001)	(00010)	(00011)
(00100)	(00101)	(00110)	(00111)
(01000)	(01001)	(01010)	(01011)
(01100)	(01101)	(01110)	(01111)
(10000)	(10001)	(10010)	(10011)
(10100)	(10101)	(10110)	(10111)
(11000)	(11001)	(11010)	(11011)
(11100)	(11101)	(11110)	(11111)

  - These sets are linear combinations of **basis** vector or **spanning** set (1 0 0 0 0, 0 1 0 0 0, 0 0 1 0 0,0 0 0 1 0, 0 0 0 0 1)

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
- ***Addition of Vectors,*** Let $\boldsymbol{v_1} = (\mathbf{1\ 0\ 1\ 1\ 1})$& $\boldsymbol{v_2} = (\mathbf{1\ 1\ \ 0\ \ 0\ 1})$
  - The vector sum of $\boldsymbol{v_1}\&\boldsymbol{v_2}$ is $(10111) + (11001) = (1 + 1,0 + 1,1 + 0,1 + 1) = (01110)$.
- ***Scalar multiplication*** with vectors, Let “0” & “1” are the scalar

$$0.(11010) = (0.1,0.1,0.0,0.1,0.0) = (00000),$$
$$1.(11010) = (1.1,1.1,1.0,1.1,1.0) = (11010),$$

  - The vector space of all n-tuples over any field *F* constructed in a similar manner.
  - However, we are mostly concerned with the vector space of all *n-tuples* over GF(2) or over an extension field of GF(2) [e.g. GF(2^m)].
  - Because *V* is a vector space over a field *F*, it may happen that subset *S* of *V* is also a vector space over *F*.
  - Such a subset is called a *subspace* of *V.*

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
  - Let *S* be a nonempty subset of a vector space *V* over a field *F* then, *S* is a subspace of V if the following conditions are satisfied;
  - For any two vectors **u** & **v** in *S,* **u + v** also a vector in *S.*
  - For any element a in F & any vector **u** in *S,* **a.u** is also in *S.*
  - Consider the vector space of all 5 tuple over GF(2) the set

$$\{(00000),(00111),(11010),(11101)\}$$

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
- ***Linear Combination of vectors***
  - Let $v_1, v_2, \cdots, v_k$ be k vectors in vector space V over a field F, let $a_1, a_2, \cdots, a_k$ be k scalars from F. The sum of product of scalar and vector that is

$$a_1v_1 + a_2v_2 + \cdots + a_kv_k$$

  - Clearly, the sum of two linear combinations of $v_1, v_2, \cdots, v_k$.

$$(a_1v_1 + a_2v_2 + \cdots + a_kv_k) + (b_1v_1 + b_2v_2 + \cdots + b_kv_k)$$

$$= (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \cdots + (a_k + b_k)v_k$$

- ***Scalar Product :***
  - The product of scalar c in F & a linear combination of $v_1, v_2, \cdots, v_k$.

$$c\,.(a_1v_1 + a_2v_2 + \cdots + a_kv_k) = (c.a_1)v_1 + (c.a_2)v_2 + \cdots + (c.a_k)v_k$$

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
  - **Statement:**
    - Let $v_1, v_2, \cdots, v_k$ be *k* vectors in vector space over a field *F*. The set of all linear combinations of $v_1, v_2, \cdots, v_k$ forms a subspace of *V.*
  - **Proof:**
    - A set of vectors $v_1, v_2, \cdots, v_k$ in a vector space V over a field F said to be linearly dependent if and only if there exist k scalars $a_1, a_2, \cdots, a_k$ from field F, not all zero, such that

$$a_k v_1 + a_k v_2 + \cdots + a_k v_k = 0$$

  - A set of vectors $v_1, v_2, \cdots, v_k$ is said to be ***linearly independent*** if it is not ***linearly dependent.***

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
  - That is $v_1, v_2, \cdots, v_k$ are **linearly independent**. If and only if

$$a_k v_1 + a_k v_2 + \cdots + a_k v_k \neq 0$$

  - Unless $a_1 = a_2 = \cdots = a_k = 0$.
  - **Example:**
    - Consider the vector space of all 5-tuple over GF(2) the **linear combinations** of (00111) & $(11101)$are

$$0.(00111) + 0.(11101) = (00000)$$
$$0.(00111) + 1.(11101) = (11101)$$
$$1.(00111) + 0.(11101) = (00111)$$
$$1.(00111) + 1.(11101) = (11010)$$

Set of vectors are linearly independent

Modern Algebra…

- ***Vector Spaces V_n :***
  - **Example:**
    - The vectors (10110) , (01001), & (11111) are **linearly dependent**. Since

$$1\,.\,(10110) + 1.\ (01001) + 1.\,(11111) = (00000);$$

    - However, (10110) , (01001), & (11111) are linearly independent.

    - All eight combinations of these vectors are given here:

$$
\begin{aligned}
0\,.\,(10110) + 0.\ (01001) + 0.\,(11111) &= (00000),\\
0\,.\,(10110) + 0.\ (01001) + 1.\,(11111) &= (11011),\\
0\,.\,(10110) + 1.\ (01001) + 0.\,(11111) &= (01001),\\
0\,.\,(10110) + 1.\ (01001) + 1.\,(11111) &= (10010),\\
1\,.\,(10110) + 0.\ (01001) + 0.\,(11111) &= (10110),\\
1\,.\,(10110) + 0.\ (01001) + 1.\,(11111) &= (01101),\\
1\,.\,(10110) + 1.\ (01001) + 0.\,(11111) &= (11111),\\
1\,.\,(10110) + 1.\ (01001) + 1.\,(11111) &= (00100),
\end{aligned}
$$

A set of vectors is said to ***span*** a vector space *V* if every vector in *V* is a linear combination of vectors in set .

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
  - ***Basis Vector***
  - In any vector space or subspace there exist at least one set B of linearly independent vectors that span the space.
  - This is called as a ***basis*** *(or base)*of the vector space.
  - The number of vectors in a **basis** of a vector space is called as the ***dimension*** of the vector space.
  - Consider a vector space V_n of all *n-tuples* over *GF(2)*.
  - Let us form the following n, *n-tuples*:

$$
\begin{aligned}
e_0 &= (1, 0, 0, 0, \cdots, 0, 0) \\
e_1 &= (0, 1, 0, 0, \cdots, 0, 0) \\
&\vdots \\
e_{n-1} &= (0, 0, 0, 0, \cdots, 0, 1)
\end{aligned}
$$

Linearly independent hence form all vectors in vector space *Vn*

Modern Linear Abstract Algebra

- ***Vector Spaces V_n :***
  - Where the *n-tuple* $\mathbf{e}_i$ has only one nonzero component at the i^{th} position.
  - Then every *n-tuple* $(a_0, a_1, a_2, \cdots, a_{n-1})$ in V_n can be expressed as a linear combination of $e_0, e_1, \cdots, e_{n-1}$ as follows:

$$(a_0, a_1, a_2, \cdots, a_{n-1}) = a_0 e_0 + a_1 e_1 + a_2 e_2 + \cdots + a_{n-1} e_{n-1} .$$

  - Therefore $e_0, e_1, \cdots, e_{n-1}$ span the vector space V_n of n-tuple over *GF(2)*.
  - We also see that $e_0, e_1, \cdots, e_{n-1}$ are linearly independent.
  - Hence, they form a basis for V_n, & dimension of V_n is n.
  - If $k < n$ & $v_1, v_2, \cdots, v_k$ are k linearly independent vectors in V_n, then all the linear combinations of $v_1, v_2, \cdots, v_k$ of the form, $\boldsymbol{u} = c_1 \boldsymbol{v}_1 + c_2 \boldsymbol{v}_2 + \cdots + c_n \boldsymbol{v}_n$ form a k- dimensional subspace *S of* V_n.

Modern Linear Abstract Algebra

➢ *Vector Spaces V_n :*

- ➢ Because of each c_i has two possible values 0 or 1, there are 2^k possible distinct linear combinations of $v_1, v_2, \ldots, v_k$.
- ➢ Thus, *S* consists of 2^k vectors and is a k-dimensional subspace of V_n.
- ➢ Let $\boldsymbol{u} = (u_1, u_2, \cdots, u_{n-1})$ & $\boldsymbol{v} = (v_1, v_2, \cdots, v_{n-1})$ be two *n-tuples* in V_n.
- ➢ We define the *inner product or (dot product)* of ***u*** & ***v*** as:

$$\boldsymbol{u}.\boldsymbol{v} = u_0.v_0 + u_1.v_1 + \cdots + u_{n-1}.v_{n-1}$$

- ➢ Where $u_i.v_i$ & $u_i.v_i + u_{i+1}.v_{i+1}$ are carried out in modulo-2 multiplication & addition.
- ➢ Hence, inner product of $u_i.v_i$ is a scalar in *GF(2)*.
- ➢ If $\boldsymbol{u}.\boldsymbol{v} = 0$, ***u*** & ***v*** are said to be *orthogonal* to each other.

Modern Linear Abstract Algebra

- **Vector Spaces V_n :**
  - ***Statement:***
    - Let *S* be a k-dimensional subspace of the vector space Vn of *n-tuple* over *GF(2)*.
    - The dimension of its null space S*d* is in n-k. in other words ,

$$dim(S) + \dim(S_d) = n$$

- ***Irreducible polynomial:***
  - For a polynomial $f(X)$ over $GF(2)$, if polynomial has an even number of terms, it is devisable by $X + 1$.
  - A polynomial $p(X)$ over $GF(2)$ of degree m is said to be *irreducible* over $p(X)$. If it is not divisible by any polynomial over $GF(2)$ of degree less than m but greater than zero.

- ***Irreducible polynomial P(X):***
  - Among the four polynomials of degree 2, X^2, X^2+1, $\&$ X^2+X are not irreducible, since they are divisible by X or $\mathrm{X}+1$;
  - However, X^2+X+1 does not have either 0 or 1 as a root & so is not divisible by any polynomial of degree 1.
  - Therefore X^3+X+1 is not divisible by $X\ or\ X\ +\ 1$.
  - Therefore, X^2+X+1 is an irreducible polynomial of degree 2.
  - The polynomial X^3+X+1 is an irreducible polynomial of degree 3.
  - X^3+X+1 is neither divisible by any polynomial of degree 1, nor any polynomial of degree 2 or higher except itself

Primitive Polynomial

- Verify whether irreducible polynomial $P(X) = X^4 + X^3 + X^2 + X + 1$ over GF(2)={0,1} is primitive or not

- $P(X)$, must divide $X^{15} + 1$ over GF(2)={0,1}

- Also, check whether $P(X)$ divides $X^5 + 1$

Modern Linear Abstract Algebra

- An ***irreducible polynomial*** *P(X*) of degree m is said to be ***primitive*** if the smallest positive integer n for which p(X) divides X^n+1 where, $n=2^m-1$
- For Example Consider *P(X)=* X^3+X+1 *is* irreducible polynomial over GF(2)

$$
\begin{array}{r|l}
 & X^4 + X^2 + X + 1 \\
\hline
X^3+X+1 & X^7 + 1 \\
 & X^7 + X^5 + X^4 \\
\cline{2-2}
 & X^5 + X^4 + 1 \\
 & X^5 + X^3 + X^2 \\
\cline{2-2}
 & X^4 + X^3 + X^2 + 1 \\
 & X^4 + X^2 + X \\
\cline{2-2}
 & X^3 + X + 1 \\
 & X^3 + X + 1 \\
\cline{2-2}
 & 0.
\end{array}
$$

- Primitive Polynomial help us to construct the Extension field of irreducible polynomial P(X) where its roots exist.

Primitive Polynomial

- Verify whether irreducible polynomial $P(X) = X^4 + X^3 + X^2 + X + 1$ over GF(2)={0,1} is primitive or not

- P(X), must divide $X^{15} + 1$ over GF(2)={0,1}

- Also, check whether P(X) divides $X^5 + 1$

Primitive Polynomial

$X^4+X^3+X^2+X+1)\ X^{15} \quad + \quad 1 \qquad (\ X^{11} + X^{10} \ldots$

$X^{15} + X^{14} + X^{13} + X^{12} + X^{11}$

$X^{14} + X^{13} + X^{12} + X^{11} + 1$

.

.

0

Primitive Polynomial

- $X^4+X^3+X^2+X+1) \quad X^5 \quad + \quad 1 \quad (X + 1$

$$
\begin{array}{r}
- \quad X^5 + X^4 + X^3 + X^2 + X \\
\text{------------------------------} \\
X^4 + X^3 + X^2 + X + 1 \\
- \quad X^4 + X^3 + X^2 + X + 1 \\
\text{------------------------------} \\
0
\end{array}
$$

Hence, P(X)= $X^4 + X^3 + X^2 + X + 1$ is irreducible polynomial over GF(2) but not primitive

Modern Linear Abstract Algebra

- ***Extension field GF(2^m):*** **(Where m is the degree of irreducible polynomial)**
  - Let m = 4, the polynomial $p(X) = 1 + X + X^4$ is a primitive polynomial over GF(2), set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$.
  - α is the primitive element, exist in the extension field GF(2^m) of GF(2).
  - Then $\propto^4 = 1 + \propto$, using this relation, we can construct $GF(2^4)$.
  - The identity $\propto^4 = 1 + \propto$ is used repeatedly to form the polynomial representation for the element of $GF(2^4)$.

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

Modern Linear Abstract Algebra

- To multiply two elements α^i & α^j, we simply add their exponent & use fact that $\alpha^{15} = 1$.
- For Example $\alpha^5 . \alpha^7 = \alpha^{12}$ & $\alpha^{12}. \alpha^7 = \alpha^{19} = \alpha^4$,
- Dividing $\alpha^j \; by \; \alpha^i$, we simply multiply $\alpha^j$by multiplicative invers α^{15-i} for α^i .
- For example $\alpha^4/_{\alpha^{12}} = \alpha^4 . \alpha^3 = \alpha^7$ & $\alpha^{12}/_{\alpha^5} = \alpha^{12}. \alpha^{10} = \alpha^{22} = \alpha^7$.
- To add α^i & α^j, we use their polynomial representation given thus.

$$\alpha^5 + \alpha^7 = (\alpha + \alpha^2) + (1 + \alpha + \alpha^3) = 1 + \alpha^2 + \alpha^3 = \alpha^{13},$$

$$1 + \alpha^5 + \alpha^{10} = 1 + (\alpha + \alpha^2) + (1 + \alpha + \alpha^2) = 0.$$

Modern Linear Abstract Algebra

- ***Extension field GF(2^m): (Where m is the degree of irreducible polynomial)***
  - Table 1 : All 16 elements of GF(16) i.e. GF(2^4) are given in power of α, polynomial form of α & 4 tuple form (binary form) is given

Power representation	Polynomial representation	4-Tuple representation
0	0	(0 0 0 0)
1	1	(1 0 0 0)
α	α	(0 1 0 0)
α^2	α^2	(0 0 1 0)
α^3	α^3	(0 0 0 1)
α^4	$1+\alpha$	(1 1 0 0)
α^5	$\alpha+\alpha^2$	(0 1 1 0)
α^6	$\alpha^2+\alpha^3$	(0 0 1 1)
α^7	$1+\alpha+\alpha^3$	(1 1 0 1)
α^8	$1+\alpha^2$	(1 0 1 0)
α^9	$\alpha+\alpha^3$	(0 1 0 1)
α^{10}	$1+\alpha+\alpha^2$	(1 1 1 0)
α^{11}	$\alpha+\alpha^2+\alpha^3$	(0 1 1 1)
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	(1 1 1 1)
α^{13}	$1+\alpha^2+\alpha^3$	(1 0 1 1)
α^{14}	$1+\alpha^3$	(1 0 0 1)

Modern Linear Abstract Algebra

- ***Factorization of X^n + 1 over GF(2), where n =2^m-1***
  - Let $f(x)$ be a polynomial with coefficients from GF(2). Let β be an element in extension field $\mathrm{GF}(2^m)$.
  - If β is a root of $f(x)$, then for any l $\geq 0, \beta^2$ is also a root of $f(x)$.
  - The element β^{2l} is called a *conjugate of* β.
  - The $2^m + 1$ nonzero elements of GF(2) from all the roots of $x^{2m-1} + 1$.
  - The element of GF(2^m) form all the roots of $x^{2m} + x$.
  - Let $\emptyset(x)$ be the polynomial of smallest degree over GF(2) such that $\emptyset(\beta) = 0$. The $\emptyset(x)$ is called the *minimal polynomial* of β, $\emptyset(x)$ is unique.
  - The minimal polynomial $\emptyset(x)$ of the field element β is irreducible.

Construction of GF(16)

- $GF(2^4)=GF(16) = \{0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3,$
  $\alpha + 1,\ \alpha^2 + \alpha,\ \alpha^3 + \alpha^2,\ \alpha^3 + \alpha + 1,$
  $1 + \alpha^2,\ \alpha^3 + \alpha,\ \alpha^2 + \alpha + 1,\ \alpha^3 + \alpha^2 + \alpha,$
  $\alpha^3 + \alpha^2 + \alpha + 1,\ \alpha^3 + \alpha^2 + 1,\ \alpha^3 + 1\}$

- $GF(2^4)=GF(16) = \{\mathbf{0},\ \alpha^0,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6,\ \ldots\ldots,\ \alpha^{14}\}$

- Find the primitive elements from the GF(16) ?

Irreducible Polynomial over GF(2) & Extension Fields

- $\alpha^5 = \alpha^3 + \alpha^2 = 1 + \alpha + \alpha^2$

- $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = 1 + \alpha^2$
- $\alpha^7 = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1$

- $GF(2^3) = GF(8) = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, 1 + \alpha^2\}$
- $GF(2^3) = GF(8) = \{0, 1, \alpha, \alpha^2, \ldots\ldots, \alpha^6\}$
- Find the additive and Multiplicative inverse of each elements from extension Field

Modern Linear Abstract Algebra

- ***Factorization of X^n + 1 over GF(2), where n =2^m-1***
  - Consider the Galois fields GF(16), Let $\beta = \alpha^3$.
  - The conjugates of β are

$$\beta^{2^1} = \alpha^6. \quad \beta^{2^2} = \alpha^{12}. \quad \beta^{2^3} = \alpha^{24} = \alpha^9.$$

  - The minimal polynomial of $\beta = \alpha^3$ is then

$$\emptyset(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9)$$

  - Multiplying out the right hand side of proceeding equation, obtain,

$$\emptyset(X) = [X^2 + (\alpha^3 + \alpha^6)X + \alpha^9][X^2 + (\alpha^{12} + \alpha^9)X + \alpha^{21}]$$

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

$$= X^4 + (\alpha^2 + \alpha^8)X^3 + (\alpha^6 + \alpha^{10} + \alpha^9)X^2 + (\alpha^{17} + \alpha^8) + \alpha^{15}$$

Modern Linear Abstract Algebra

- ***Factorization of X^n + 1 over GF(2), where n =2^m-1***
  - Consider the element $\alpha^5 \ in\ GF(16)$. Since the $(\alpha^5)^{2^2} = \alpha^{20} = \alpha^5$,
  - The only conjugate of α^5 is α^{10}, Both α^5 & α^{10} both have order n =3 . The minimal polynomial of α^5 & α^{10} is $X^2 + X + 1$. Whose degree is factor of m = 4.
  - The conjugates of α^3 are α^6, α^9, & α^{12}, They all have order m =5.
  - The conjugates for α^7 are α^{11} , α^{13} ,α^{14} , The minimal polynomial for α^7 is:

$$(X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14})$$
$$= [X^2 + (\alpha^7 + \alpha^{11})X + \alpha^{18}][X^2 + (\alpha^{13} + \alpha^{14})X + \alpha^{27}]$$
$$= (X^2 + \alpha^8 X + \alpha^3)(X^2 + \alpha^2 X + \alpha^{12})$$
$$= X^4 + (\alpha^8 + \alpha^2)X^3 + (\alpha^{12} + \alpha^{10} + \alpha^3)X^2 + (\alpha^{20} + \alpha^5)\mathrm{X} + \alpha^{15}$$
$$= X^4 + X^3 + 1$$

Modern Linear Abstract Algebra

- ***Factorization of X^n + 1 over GF(2), where n =2^m-1***
  - The conjugecy class of each element from GF(16) and corresponding polynomial are given in the table below.
  - There fore the polynomial corresponding to elements of GF(16) except zero is as follows.

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

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

Modern Linear Abstract Algebra

➢ *Factorization of X^n + 1 over GF(2) where n =2^m-1*

- The systematic (n, k) cyclic code is a sub class of linear block code which are constructed using generator polynomial of degree n-k.
- Parity check polynomial of degree **k,** where n-is codeword length,

  k- message length.

$$X^n + 1 = g(X).h(X).$$

- **Theorem 1:**
  - The generator polynomial g(*X*) of an (n , k) cyclic code is a factor of $X^n + 1$, where n =$2^m - 1$.
- **Theorem 2:**
  - If g(*X*) is a polynomial of degree (n-k) and is a factor of $X^n + 1$, then g(*X*) generates an (n , k) cyclic code *where n =*2^m*-1*

Research journals paper and Conference paper

- What is research?

- How to find research problem?

- What are Research Journal papers?

- What are Research Conference papers?

Journals

- IEEE Journals (Domain/specilization specific)
- IET Journals
- Elsevier Journals
- Springer Journals
- Inder science Journals
- Science Direct Journals
- Hindavi Journals

Conferences

- IEEE Conferences (Domain specific)
- IET Conferences
- Elsevier Conferences
- Springer Conferences
- Inder science Conferences
- Science Direct Conferences
- Hindavi Conferences

Journals

- International Journals
- National Journals
- Open access Journals
- Paid journals

- Local journals
- Local conferences

Patents, IPR

- Plagiarism check
- Patents filling
- IPR

Lab works

1. Implementation of Hamming code encoder
2. Implementation of Hamming code decoder
3. Find whether given polynomial is primitive
4. Construction of extension field
5. Find the primitive elements from the set
6. Prepare additive and multiplicative table
7. Factorization $X^n + 1$
8. Construct generator polynomial for (n,k) cyclic code
9. Construct generator matrix from Generator polynomial in systematic form
10. Implementation of cyclic code encoder
11. Implementation of cyclic code decoder
12. Implementation of LDPC code encoder
13. Implementation of LDPC code decoder

Lab works

10. Implementation of BCH encoder
11. Implementation of BCH code decoder
12. Implementation of convolutional code encoder
13. Implementation of convolutional code decoder

Primitive elements From a Set

- $GF(2^3)=GF(8) = \{0,\ 1,\ \alpha,\ \alpha^2,\ \alpha + 1,\ \alpha^2 + \alpha,\ \alpha^2 + \alpha + 1,\ 1 + \alpha^2\}$

- $GF(2^3)=GF(8) = \{\mathbf{0},\ \alpha^0,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6\}$

- Find the primitive elements from the GF(8) ?

Primitive elements From a Set

Theorem

- If α is a primitive element of given set then its other primitive elements are $(\alpha)^{2^{l}}$

  where $l > 0$

- Find the primitive elements from the GF(8)

Irreducible Polynomial over GF(2) & Extension Fields

- $GF(2^3)=GF(8) = \{0, 1, \alpha, \alpha^{2,} \ldots\ldots\ldots, \alpha^6\}$
- $P(\alpha)= \alpha^3 + \alpha + 1 =0,$
- $\alpha^3 + \alpha + 1 =0$
- $\alpha^3 = \alpha + 1$
- $\alpha^0 =1$
- $\alpha^1 = \alpha$
- $\alpha^2 = \alpha^2$
- $\alpha^3 = 1 + \alpha$, mod- $\alpha^3 + \alpha + 1$ and mod-2 operation
- $\alpha^4 = \alpha + \alpha^2$

Irreducible Polynomial over GF(2) & Extension Fields

- $\alpha^5 = \alpha^3 + \alpha^2 = 1 + \alpha + \alpha^2$

- $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = 1 + \alpha^2$
- $\alpha^7 = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1$

- $GF(2^3)=GF(8) = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, 1 + \alpha^2\}$
- $GF(2^3)=GF(8) = \{0, 1, \alpha, \alpha^2, \ldots\ldots, \alpha^6\}$
- Find the primitive elements from extension Field

Primitive elements from the GF(8)

- $GF(2^3)=GF(8) = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, 1 + \alpha^2\}$

- $GF(2^3)=GF(8) = \{\mathbf{0}, \alpha^0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$

- Find the primitive elements from the GF(8) ?

Primitive elements From a Set

- Check for element α^2 *from Gf(8)*
- $(\alpha^2)^0 = 1$
- $(\alpha^2)^1 = \alpha^2$
- $(\alpha^2)^2 = \alpha^4$
- $(\alpha^2)^3 = \alpha^6$
- $(\alpha^2)^4 = \alpha^8 = \alpha$ .....$(\alpha^7 = 1)$
- $(\alpha^2)^5 = \alpha^{10} = \alpha^3$
- $(\alpha^2)^6 = \alpha^{12} = \alpha^5$

- All elements from the set are generated using α^2 hence α^2 is a primitive elements

Primitive elements from a Set

- Element α^2 for primitive therefore other primitive elements are
- $(\alpha^2)^{2l}$ *for l>0*
- *Let l =1*
- $(\alpha^2)^{2^1} = (\alpha^2)^2 = \alpha^4$
- *Let l =2*
- $(\alpha^2)^{2^2} = \alpha^8 = \alpha$
- *Let l =3*
- $(\alpha^2)^{2^3} = \alpha^{16} = \alpha^2$ ....repeating
- Hence if α^2 is primitive element from the set then other primitive elements are α α^4
- We know that α is a primitive element in the extension field , therefore other primitive elements are α^2 α^4

Primitive elements from a Set

- Check for element α^3 *from Gf(8)*
- $(\alpha^3)^0 = 1$
- $(\alpha^3)^1 = \alpha^3$
- $(\alpha^3)^2 = \alpha^6$
- $(\alpha^3)^3 = \alpha^9 = \alpha^2$
- $(\alpha^3)^4 = \alpha^{12} = \alpha^5$ .....$(\alpha^7 = 1)$
- $(\alpha^3)^5 = \alpha^{15} = \alpha$ .....$(\alpha^7 = 1)$
- $(\alpha^3)^6 = \alpha^{18} = \alpha^4$

- All elements from the set are generated using α^3 hence α^3 is a primitive elements

- Element α^3 for primitive therefore other primitive elements are
- $(\alpha^3)^{2l}$ *for l>0*
- *Let l =1*
- $(\alpha^3)^{2^1} = (\alpha^3)^2 = \alpha^6$
- *Let l =2*
- $(\alpha^3)^{2^2} = \alpha^{12} = \alpha^5$
- *Let l =3*
- $(\alpha^3)^{2^3} = \alpha^{24} = \alpha^3$ ....repeating
- Hence if α^3 is primitive element from the set then other primitive elements are α^5 and α^6

Primitive Elements of GF(8)

- Hence α, α^2 , α^3 α^4 α^5 α^6 are primitive element from the Extension field GF(8)

Binary Representation of Polynomial

- $GF(2^3)=GF(8) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$

- $GF(2^3)=GF(8) = \{0, 1, \alpha, \alpha^2, 1+\alpha, \alpha+\alpha^2, 1+\alpha+\alpha^2, 1+\alpha^2\}$

- $GF(2^3)=GF(8) = \{000, 100, 010, 001, 110, 011, 111, 101\}$

Roots of a Polynomial P(X)

- GF(2^3)=GF(8) = {0, 1, α, α^2 , $\alpha + 1$, $\alpha^2 + \alpha$, $\alpha^2 + \alpha + 1$, $1 + \alpha^2$ }

- GF(2^3)=GF(8) = {0, α^0, α ,α^2 , α^3, α^4, α^5, α^6}

- Theorem
- If α is a root of a polynomial then its other roots are $(\alpha)^{2^l}$, where l>0

Roots of a Polynomial P(X)

- α is a root of polynomial then its other roots are $(\alpha)^{2^l}$, where l>0
- Let l=1,2,3...
- α^2 , α^4 , $\alpha^8 = \alpha$ ....(α^7 =1)
- Hence the elements α , α^2 , α^4 forms the conjugacy class and the
- Polynomial corresponding to above root is
- P(X) = (X- α) (X- α^2) (X- α^4)

Roots of a Polynomial P(*X*)

- $P(X) = [\, X2 - X\,\alpha 2 - X\,\alpha - \alpha 3\,]\,(X - \alpha 4)$
- $= x3 - x2\,\alpha 4 - x2\,\alpha 2 - x\,\alpha 6 - x2\,\alpha - x\,\alpha 5 - x\,\alpha 3 +$

  $\alpha 7$

- $= x3 - x2\,(\alpha 4 + \alpha 2 + \alpha) - x\,(\alpha 6 + \alpha 5 + \alpha 3) + 1$
- $P_{\alpha}(X) = x3 + 0 + X + 1$
- $P_{\alpha}(X) = X3 + X + 1$
- *It is also called as Minimal polynomial of elements* $\alpha^2 , \alpha^4 , \alpha$

Roots of a Polynomial P(X)

- GF(2^3)=GF(8) = {0, 1, α, α^2 , $\alpha + 1$, $\alpha^2 + \alpha$, $\alpha^2 + \alpha + 1$, $1 + \alpha^2$ }

- GF(2^3)=GF(8) = {**0**, α^0, α ,α^2 , α^3, α^4, α^5, α^6}

- Let α^3 be the root of polynomial then its other root are

- $(\alpha^3)^{2^l}$ are ??

- P $\alpha^3(X)$= ?

Roots of a Polynomial P(*X*)

- Let α^3 be the root of polynomial then its other root are obtained by using $(\alpha^3)^{2^l}$
- Let l =1 , then $(\alpha^3)^{2^1}$ is α^6
- Let l =2 , then $(\alpha^3)^{2^2}$ is $\alpha^{12} = \alpha^7 \cdot \alpha^5 = 1 \cdot \alpha^5$
- Let l =3 , then $(\alpha^3)^{2^3}$ is $\alpha^{24} = \alpha^{21} \cdot \alpha^3 = \alpha^3$

  (repeating)
- Hence α^3 , α^6 , α^5 are the elements in conjugacy class

- Hence polynomial corresponding to above root is
- $P(X) = (X- \alpha^3)(X- \alpha^6)(X- \alpha^5)$
- $P_{\alpha^3}(X) =$?

Factorization of $X^n + 1$

- $P_{\alpha^3}(X) = [(X-\alpha^3)(X-\alpha^6)](X-\alpha^5)$
- $P_{\alpha^3}(X) = [(X2 - X\alpha^6 - X\alpha^3 + \alpha^9)](X-\alpha^5)$
- $P_{\alpha^3}(X) = [(X3 - X2\alpha^5 - X2\alpha^6 - X\alpha^{11} - X2\alpha^3 + X\alpha^{8+}$ $X\alpha^{9-}\alpha^{14}]$
- $P_{\alpha^3}(X) = [(X3 - X2(\alpha5+\alpha6+\alpha3) + x(\alpha11+\alpha8+\alpha9)+1]$
- $P_{\alpha^3}(X) = [(X3 - X2(1) + x(0)+1]$
- $P_{\alpha^3}(X) = x3 + X2 + 1$
- x

Factorization of $X^n + 1$

- $X^7 + 1 = P\alpha^3(X) \cdot P\alpha(X) \cdot P\alpha^0(X)$
- $X^7 + 1 = (X+1)(x3 + X2 + 1).(x3 + X + 1)$
- Verify, $X^7 + 1 = (X+1)(x3 + X2 + 1).(x3 + X + 1)$

Factorization of $X^n + 1$

- $GF(2^3) = GF(8) = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, 1 + \alpha^2\}$
- Verify polynomial corresponding to GF(8) is $X(X^7 + 1)$ where $n = 2^m - 1$
- If we exclude zero element then it will be GF(7) and
- The corresponding polynomial will be $X^7 + 1$
- We can obtain it as follows-

Factorization of $X^n + 1$

- GF(8) will be
- $P(X) = (X - 0)(X - \alpha^0)(X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^0)(X - \alpha^5)$ $(X - \alpha^6) = X(X^7 + 1)$

- GF(7) will be
- $P(X) = (X - \alpha^0)(X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^0)(X - \alpha^5)(X - \alpha^6)$
- $= (X^7 + 1)$

Construction GF(16)

- Consider $P(x) = X^4 + X + 1$
- and α as primitive element from extension field
- $\alpha^0 = 1$
- $\alpha^1 = \alpha$
- $\alpha^2 = \alpha^2$
- $\alpha^3 = \alpha^3$
- $\alpha^4 = \alpha + 1$
- $\alpha^5 = \alpha^2 + \alpha$

Construction GF(16)

- $\alpha^6 = \alpha^3 + \alpha^2$
- $\alpha^7 = \alpha^3 + \alpha + 1$ .....$(\alpha^4 = \alpha^3 + \alpha + 1)$
- $\alpha^8 = \alpha^4 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = 1 + \alpha^2$
- $\alpha^9 = \alpha^3 + \alpha$
- $\alpha^{10} = 1 + \alpha + \alpha^2$
- $\alpha^{11} = \alpha + \alpha^2 + \alpha^3$
- $\alpha^{12} = \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^2 + \alpha^3$
- $\alpha^{13} = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha + \alpha + \alpha^2 + \alpha^3$
  $= 1 + \alpha^2 + \alpha^3$
- $\alpha^{14} = \alpha + \alpha^3 + \alpha^4 = 1 + \alpha + \alpha + \alpha^3 = 1 + \alpha^3$
- $\alpha^{15} = \alpha + \alpha^4 = 1 + \alpha + \alpha = 1$

Construction of GF(16)

- $GF(2^4)=GF(16) = \{0, 1, \alpha, \alpha^2, \alpha^3,$
  $\alpha + 1, \alpha^2 + \alpha, \alpha^3 + \alpha^2, \alpha^3 + \alpha + 1,$
  $1 + \alpha^2, \alpha^3 + \alpha, \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha,$
  $\alpha^3 + \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + 1, \alpha^3 + 1\}$

- $GF(2^4)=GF(8) = \{\mathbf{0}, \alpha^0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \ldots, \alpha^{14}\}$

- Find the minimal polynomial of each elements

Modern Linear Abstract Algebra

- ***Factorization of X^n + 1 over GF(2), where n =2^m-1***
  - Consider the Galois fields GF(16), Let $\beta = \alpha^3$.
  - The conjugates of β are

$$\beta^{2^1} = \alpha^6. \quad \beta^{2^2} = \alpha^{12}. \quad \beta^{2^3} = \alpha^{24} = \alpha^9.$$

  - The minimal polynomial of $\beta = \alpha^3$ is then

$$\emptyset(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9)$$

  - Multiplying out the right hand side of proceeding equation, obtain,

$$\emptyset(X) = [X^2 + (\alpha^3 + \alpha^6)X + \alpha^9][X^2 + (\alpha^{12} + \alpha^9)X + \alpha^{21}]$$

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

$$= X^4 + (\alpha^2 + \alpha^8)X^3 + (\alpha^6 + \alpha^{10} + \alpha^9)X^2 + (\alpha^{17} + \alpha^8) + \alpha^{15}$$

Minimal polynomial

- $\alpha^3 + \alpha^6 = \alpha^3 + \alpha^3 + \alpha^2$
- $= \alpha^2$
- $\alpha^{12} + \alpha^9 = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^3 + \alpha$

$= 1 + \alpha^2$

$= \alpha^8$

$\alpha^{21} = \alpha^6$

Minimal polynomial

- $\alpha^8 + \alpha^2 = 1 + \alpha^2 + \alpha^2 = 1$
- $\alpha^6 + \alpha^{10} + \alpha^9 = \alpha^3 + \alpha^2 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha$
- $= 1$
- $\alpha^{17} + \alpha^8 = \alpha^2 \,.\, \alpha^{15} + \alpha^8$
- $= \alpha^2 \,.\, 1 + 1 + \alpha^2$

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

$= 1$

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

The minimal polynomial of the element α^3 is given by

$\boldsymbol{\Phi_{\alpha 3}(x) = X^4 + X^3 + X^2 + X + 1}$

$\boldsymbol{P_{\alpha 3}(x) = X^4 + X^3 + X^2 + X + 1}$

Hence minimal polynomial of the element α^3, α^6, α^9, α^{12} is same

Modern Linear Abstract Algebra

- ***Factorization of X^n + 1 over GF(2), where n =2^m-1***
  - Consider the element $\alpha^5\ in\ GF(16)$. Since the $(\alpha^5)^{2^2} = \alpha^{20} = \alpha^5$,
  - The only conjugate of α^5 is α^{10}, Both α^5 & α^{10} both have order n =3 . The minimal polynomial of α^5 & α^{10} is $X^2 + X + 1$. Whose degree is factor of m = 4.
  - The conjugates of α^3 are α^6, α^9, & α^{12}, They all have order m =5.
  - The conjugates for α^7 are α^{11} , α^{13} ,α^{14} , The minimal polynomial for α^7 is:

$$
\begin{aligned}
&(X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}) \\
&= [X^2 + (\alpha^7 + \alpha^{11})X + \alpha^{18}][X^2 + (\alpha^{13} + \alpha^{14})X + \alpha^{27}] \\
&= (X^2 + \alpha^8 X + \alpha^3)(X^2 + \alpha^2 X + \alpha^{12}) \\
&= X^4 + (\alpha^8 + \alpha^2)X^3 + (\alpha^{12} + \alpha^{10} + \alpha^3)X^2 + (\alpha^{20} + \alpha^5)\mathrm{X} + \alpha^{15} \\
&= X^4 + X^3 + 1
\end{aligned}
$$

Minimal polynomial

- $\alpha^8 + \alpha^2 = 1 + \alpha^2 + \alpha^2 = 1$
- $\alpha^{12} + \alpha^{10} + \alpha^3 = 1 + \alpha + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3$

  $= 0$
- $\alpha^{20} + \alpha^5 = \alpha^{15} . \alpha^5 + \alpha^5$
- $= 1. \alpha^5 + \alpha^5$
- $= \alpha^5 + \alpha^5$
- $= 0$

Minimal polynomial

$P(x) = (X - \alpha^5).(X - \alpha^{10})$

$= [X^2 - (\alpha^5 + \alpha^{10}) X + \alpha^{15}]$

$P_{\alpha 5}(x) = X^2 + X + 1$

Hence ,

$P_{\alpha 5}(x) = X^2 + X + 1$

$\mathbf{P_{\alpha 3}(x) = X^4 + X^3 + X^2 + X + 1}$

$\mathbf{P_{\alpha 7}(x) = X^4 + X^3 + 1}$

$\mathbf{P_{\alpha}(x) = X^4 + X + 1}$

$\mathbf{P_{\alpha 0}(x) = X + 1}$

$\mathbf{P_{\alpha -\infty}(x) = X}$

Modern Linear Abstract Algebra

- ***Factorization of X^n + 1 over GF(2), where n =2^m-1***
  - The conjugecy class of each element from GF(16) and corresponding polynomial are given in the table below.
  - There fore the polynomial corresponding to elements of GF(16) except zero is as follows.

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

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

Factorization of $X^n + 1$

- $X^{15} + 1 = P_{\alpha 0}(x).\ P_{\alpha 3}(x).\ P_{\alpha 7}(x).\ P_{\alpha}(x).\ P_{\alpha 5}(x)$

- $X^{15} + 1 = (X + 1).\ (X^4 + X^3 + X^2 + X + 1).$
  $(X^4 + X^3 + 1).\ (X^4 + X + 1).\ (X^2 + X + 1)$

- **Find the generator polynomial for (n , k) linear cyclic code**
- **Consider i) n=15 , k=11**
- **ii) n=15 , k=4**
- **iii) n=15, k=7**
- **iv) n=15, k=8**

- Hence find parity check polynomial h(X)
- **Consider i) n=15 , k=11**
- **ii) n=15 , k=4**
- **iii) n=15, k=7**
- **iV) n=15, k=8**

- $X^{15} + 1 = (X + 1).(X^4 + X^3 + X^2 + X + 1).$
  $(X^4 + X^3 + 1).(X^4 + X + 1).(X^2 + X + 1)$

- $X^{15} + 1 = g(X).h(X)$

Construct matrix from generator polynomial

- $g(X)=1+x+x^3$ (7,4)

- 1 1 0 1 0 0 0
- G= 0 1 1 0 1 0 0 ………………….(1)
- 0 0 1 1 0 1 0
- 0 0 0 1 1 0 1
- Convert G matrix in systematic form
- Construct H Matrix from G
- Implement Hamming decoder
- Problem 1
- Obtain encoding sequence for (7,4) code with message bits 1 0 0 1 and take generator matrix in systematic form by converting from equ. 1

Construction of GF(16)

- $GF(2^4)=GF(16) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha + 1, \alpha^2 + \alpha, \alpha^3 + \alpha^2, \alpha^3 + \alpha + 1, 1 + \alpha^2, \alpha^3 + \alpha, \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + 1, \alpha^3 + 1\}$

- $GF(2^4)=GF(8) = \{\mathbf{0}, \alpha^0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \ldots\ldots, \alpha^{14}\}$

- Find the primitive elements from the GF(16) ?

Primitive elements From a Set

- Check for element α^2 *from Gf(16)*
- $(\alpha^2)^0 = 1$
- $(\alpha^2)^1 = \alpha^2$
- $(\alpha^2)^2 = \alpha^4$
- $(\alpha^2)^3 = \alpha^6$
- $(\alpha^2)^4 = \alpha^8$
- $(\alpha^2)^5 = \alpha^{10}$
- $(\alpha^2)^6 = \alpha^{12}$
- $(\alpha^2)^7 = \alpha^{14}$
- $(\alpha^2)^8 = \alpha^{16} = \alpha^1 \cdot \alpha^{15} = \alpha$
- $(\alpha^2)^9 = \alpha^{18} = \alpha^3 \cdot \alpha^{15} = \alpha^3$
- $(\alpha^2)^{10} = \alpha^{20} = \alpha^5 \cdot \alpha^{15} = \alpha^5$

Primitive elements From a Set

- $(\alpha^2)^{11} = \alpha^{22} = \alpha^7 \cdot \alpha^{15} = \alpha^7$
- $(\alpha^2)^{12} = \alpha^{24} = \alpha^9 \cdot \alpha^{15} = \alpha^9$
- $(\alpha^2)^{13} = \alpha^{26} = \alpha^{11} \cdot \alpha^{15} = \alpha^{11}$
- $(\alpha^2)^{14} = \alpha^{28} = \alpha^{13} \cdot \alpha^{15} = \alpha^{13}$
- $(\alpha^2)^{15} = \alpha^{30} = \alpha^{15} \cdot \alpha^{15} = 1$
- Therefore the element α^2 is primitive Hence the elements α^4 α^8 α are primitive as per theorem

Primitive elements from a Set

- let us check element α^2 for primitive
- $(\alpha^2)^{2^l}$ *for l>0*
- *Let l =1*
- $(\alpha^2)^{2^1} = (\alpha^2)^2 = \alpha^4$
- *Let l =2*
- $(\alpha^2)^{2^2} = \alpha^8$
- *Let l =3*
- $(\alpha^2)^{2^3} = \alpha^{16} = \alpha$
- Hence if α^2 is primitive element from the set then other primitive elements are α α^4 α^8
- We know that α is a primitive element in the extension field , therefore other primitive elements are α^2 α^4 α^8

Primitive elements from a Set

- let us check element α^3 for primitive
- $(\alpha^3)^0 = 1$
- $(\alpha^3)^1 = \alpha^3$
- $(\alpha^3)^2 = \alpha^6$
- $(\alpha^3)^3 = \alpha^9$
- .....
- ....
- $(\alpha^3)^{14} = ?$

Primitive elements from a Set

- Check for element α^3 *from Gf(16)*
- $(\alpha^3)^0 = 1$
- $(\alpha^3)^1 = \alpha^3$
- $(\alpha^3)^2 = \alpha^6$
- $(\alpha^3)^3 = \alpha^9$
- $(\alpha^3)^4 = \alpha^{12}$
- $(\alpha^3)^5 = \alpha^{15} = 1$
- $(\alpha^3)^6 = \alpha^{18} = \alpha^3 \cdot \alpha^{15} = \alpha^3$
- $(\alpha^3)^7 = \alpha^{21} = \alpha^6 \cdot \alpha^{15} = \alpha^6$

- Therefore the element α^3 is not primitive ,Hence the elements α^6 α^9 α^{12} are not primitive

Primitive elements from a Set

- let us check element α^3 for primitive
- $(\alpha^3)^{2l}$ *for l>0*
- *Let l =1*
- $(\alpha^3)^{21} = (\alpha^3)^2 = \alpha^6$
- *Let l =2*
- $(\alpha^3)^{22} = \alpha^{12}$
- *Let l =3*
- $(\alpha^3)^{23} = \alpha^{24} = \alpha^{9}$…………($\alpha^{15} = 1$)

if α^3 is not primitive element in the extension field therefore other elements α^6 α^9 α^{12} are not primitive

Primitive elements from a Set

- Check for element α^5 *from Gf(16)*
- $(\alpha^5)^0 = 1$
- $(\alpha^5)^1 = \alpha^5$
- $(\alpha^5)^2 = \alpha^{10}$
- $(\alpha^5)^3 = \alpha^{15} = 1$
- $(\alpha^5)^4 = \alpha^{20} = \alpha^5$
- $(\alpha^5)^5 = \alpha^{25} = \alpha^{10}$
- $(\alpha^5)^6 = \alpha^{30} = \alpha^{15} \cdot \alpha^{15} = 1$ (repeating)

.

.

.

- Therefore the element α^5 is not primitive ,Hence the element α^{10} is not primitive

Primitive elements from a Set

- let us check element α^5 for primitive
- $(\alpha^5)^{2l}$ *for l>0*
- *Let l =1*
- $(\alpha^5)^{21} = (\alpha^5)^2 = \alpha^{10}$
- *Let l =2*
- $(\alpha^5)^{22} = \alpha^{20} = \alpha^5$........($\alpha^{15} =1$) (repeating)
-
- α^5 is not primitive element from the set then other non primitive element is α^{10}

Primitive elements From a Set

- Check for element α^7 *from Gf(16)*
- $(\alpha^7)^0 = 1$
- $(\alpha^7)^1 = \alpha^7$
- $(\alpha^7)^2 = \alpha^{14}$
- $(\alpha^7)^3 = \alpha^{21} = \alpha^{15} \cdot \alpha^6 = 1 \cdot \alpha^6 = \alpha^6$
- $(\alpha^7)^4 = \alpha^{28} = \alpha^{15} \cdot \alpha^{13} = 1 \cdot \alpha^{13} = \alpha^{13}$
- $(\alpha^7)^5 = \alpha^{35} = \alpha^{30} \cdot \alpha^5 = 1 \cdot \alpha^5 = \alpha^5$
- $(\alpha^7)^6 = \alpha^{42} = \alpha^{30} \cdot \alpha^{12} = 1 \cdot \alpha^{12} = \alpha^{12}$
- $(\alpha^7)^7 = \alpha^{49} = \alpha^{45} \cdot \alpha^4 = 1 \cdot \alpha^4 = \alpha^4$
- $(\alpha^7)^8 = \alpha^{56} = \alpha^{45} \cdot \alpha^{11} = \alpha^{11}$
- $(\alpha^7)^9 = \alpha^{63} = \alpha^3 \cdot \alpha^{60} = \alpha^3$

Primitive elements From a Set

- $(\alpha^7)^{10} = \alpha^{70} = \alpha^{10} \cdot \alpha^{60} = \alpha^{10}$
- $(\alpha^7)^{11} = \alpha^{77} = \alpha^{2} \cdot \alpha^{75} = \alpha^{2}$
- $(\alpha^7)^{12} = \alpha^{84} = \alpha^{9} \cdot \alpha^{75} = \alpha^{9}$
- $(\alpha^7)^{13} = \alpha^{91} = \alpha^{1} \cdot \alpha^{90} = \alpha^{1}$
- $(\alpha^7)^{14} = \alpha^{98} = \alpha^{8} \cdot \alpha^{90} = \alpha^{8}$
- $(\alpha^7)^{15} = \alpha^{105} = \alpha^{15} \cdot \alpha^{90} = 1$
- Therefore ,the element α^7 is primitive. Hence the elements α^{14} α^{13} α^{11} are primitive as per theorem