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

Outline

- **Modern digital communication system**
- **ECC for data transmission and storage devices**
- **Hamming Code (n, k)**
- **Parity Check Matrix H and Generator matrix G**
- **Properties of matrices**
- **Cyclic Code (n, k)**
- **Polynomial g(X) of degree n-k**
- **Parity check polynomial h(x)**
- **2^k , Valid code *C***
- ***Code rate r =k/n***

Outline

- **Modern linear abstract Algebra-**
- **Irreducible polynomial**
- **Primitive polynomial**
- **Primitive elements ?**
- **Vector spaces *V*n**
- **Vector subspaces**
- **Linear combination of vectors**
- **Dependent / Independent set of vectors**
- **Spanning set/basis vectors**
- **Groups G**
- **Fields F**

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 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 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 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 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

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k$$

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

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

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

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

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

Modern 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 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), & (11011) are linearly independent.

- All eight combinations of these vectors are given here:

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

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 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 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 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 $v_1, v_2, \dots, v_k$.
- 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 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.

Modern Algebra…

- ***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

Modern 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)

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

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