V.J.T.I

B.Tech.(ExTc)

Sub: DCS

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

- M.Tech/B.Tech/Research Scholars who want to work on following topics can work under my Guidance
- Error correcting Codes/coding theory
- Wireless Communication
- FOC / Microwave
- Micro Strip Antennas
- IOT
- Wireless Sensor Networks
- Mobile/Vehicular Adhoc Networks
- ML
- Embedded Systems/Microprocessors/Microcontroller
- Signal processing

Digital Communication system

- **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**
- **$X^n + 1 = g(X).h(X)$**
- **Parity check polynomial h(X) of degree K**
- **2^k , Valid code C**
- ***Code rate $r = k/n$***

Error Correcting Codes

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

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*
- $\boldsymbol{r}.\mathbf{H^T = 0}$ or $\mathbf{H.r^T = 0}$ mod-2 operation,
- This is the condition to check validity of received code words

Problem

- Construct G matrix for (6, 3) linear block code and corresponding parity check matrix H in systematic form
- Verify $H.G^T = 0$
- Get matrix G or H in non systematic form and convert it into systematic form
- How many valid set of code words?
- Construct all code words *C*
- What is rate of code ?

Problem

- G=[110110, 001110,010011]
- H=[101100, 011010,110001]
- $H.G^T = \mathbf{0}$ mod-2

Problem

- Let,

G=[1 1 0 1 1 0,

0 0 1 1 1 0,

0 1 0 0 1 1]

Convert it into systematic form by using elementary row transformation ?

Problem

- Let,

  G=[110110, 001110,010011]

  Convert it into systematic form
- Adding 3rd row with 1st row and
- Interchanging 2nd and 3rd rows we get
- G'=[100101,010011,001110] , in systematic form
- Verify Row space of G & G' ?

Problem

- Row space G are-
  (000000),(100101), (010011), (001110), (110110), (101011),(011101),(111000)

Row space of G' are

(000000),(100101),(010011),(001110),
(110110),(101011),(011101),(111000)

This is a three dimensional subspace of vector space V_6 of all the 6 tuples over GF(2)

Theorem

- For any (k x n) matrix G over GF(2) with k linearly independent rows, there exists an (n-k) x n matrix H over GF(2) with (n-k) linearly independent rows such that for any row g_i in G and any row h_j in H, $g_i.h_j$ =**0,** we call G is a null space of H

Primitive elements

- Primitive elements are elements by taking power which, all the elements in the set can be obtained, except zero element

- Consider the set G , find the primitive elements from the set over mod-5

  G={0, 1 , 2 , 3, 4}

•

Primitive elements

- Consider the set G , find the primitive elements from the set over mod-5

  G={0, 1 , 2 , 3, 4}

Consider element 2

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8 = 3$ mod-5

$2^4 = 1$ (repeating)

As all the elements of G are generated, 2 is primitive element of the set G

G={0, 2^0 , 2^1 , 2^2, 2^3}

Hence, element 2 is called generator of this set

- Find other elements from the set G?

Primitive Polynomial

- An irreducible polynomial is Primitive polynomial if it divides $X^n + 1$,

- Where, $n=2^m - 1$

- m is degree of irreducible polynomial over GF(2)

Irreducible and Primitive Polynomial

- Consider , $P(X) = X^4 + X + 1$ over GF(2)={0,1}

- P(0)=0 + 0 +1=1≠ 0, mod-2
- P(1)=1 + 1 +1=3=1 ≠ 0, mod-2 ≠ 0

- As given P(X) does not satisfy either 0 or 1 hence, the given polynomial is irreducible over GF(2)

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)

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

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

Non primitive polynomial

- Example of irreducible polynomial which is not primitive

- Verify whether the following polynomials are irreducible and primitive over GF(2)={0,1}

- 1. $P(X) = X^4 + X + 1$

- 2. $P(X) = X^4 + X^3 + X^2 + X + 1$