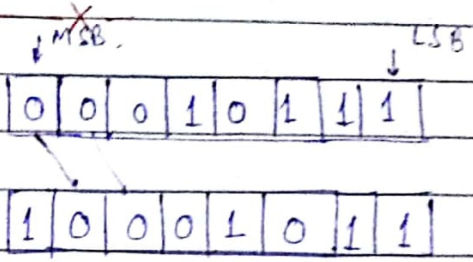
Chs:- BCH

Page No.:
Date: 19/09/17

BCH -- Bose Chaudhari Hocquenghem Codes in 1959.

BCH forms a class of cyclic error correcting words. Data constructed using polynomial over Galois field GF(n).

→ **Cyclic Codes** :-



If string 00010111. is valid codeword Apply right circular shift. gives string '10001011' which is again a codeword which is valid.

~~Again~~ By Applying Right shift, moves LSB to left most position so that it becomes MSB. & other positions are shifting one to the right corres. to original string.

Code C is cyclic if :-

(1) C is a linear code.

(2) Any cyclic shift of codeword is also a codeword.

eg :- Codeword $a_0 a_1 \ldots\ldots a_{n-1}$ is C
then $a_{n-1} a_0 a_1 \ldots\ldots a_{n-2}$ is also codeword C.

Date : / /

Constraints added to cyclic codes :-

1. Cyclic shift in codeword results in another valid codeword.

→ **Polynomials :**

$$f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots\dots a_{n-1} x^1 + a_n x^0$$

Degree of $f(x)$ is n.

Or

$$f(x) = f_0 + f_1 x + \dots\dots + f_m x^m$$

where, $x \rightarrow$ Indeterminant

& Coeff. of $f_0, f_1, f_2 \dots f_n$ are GF.

f_m = leading coeff.

$f_m \neq 0$, then m is called degree

eg :- $f(x) = 3 + 7x + x^3 + 5x^4 + x^6$

$f(x)$ is monic.

eg :- $a(x) = x^3 + x + 1$

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

under GF(2)

$$x^2+x+1 \;\overline{)}\; x^3+x+1 \quad (x+1$$

$$x^3 + x^2 + x$$

$$x^2 + 1$$

$$x^2 + x + 1$$

$$x$$

GF is used in

→ q should be prime always.

Page No.:
Date: 20/09/17

BCH: One of most powerful tool as it is known for multiple error correcting ability & ease of encoding & decoding & is powerful random error detecting.

→ Also part of linear block code.

Primitive elements :-

eg: ① GF(q) → Finite no. of elements
→ have atleast one prime element.

Primitive element of Galva field GF(q) is an element 'α' such that every field element can be expressed as a power of 'α'.

for eg: Q: Consider GF(5)

Sol: Since, q = 5. (which is prime).
∴ modulo arithmetic will work.
Consider, element 2.

Sol: P.T. 2 is primitive element.

$2^0 = 1 \pmod 5 = 1$
$2^1 = 2 \pmod 5 = 2$
$2^2 = 4 \pmod 5 = 4$
$2^3 = 8 \pmod 5 = 3$

} ∴ which are under 5

Hence, all elements of GF(5) i.e 1, 2, 3, 4 can be represented as power of 2.

P.T 3 is primitive element of

$3^0 = 1 \pmod 5 = 1$
$3^1 = 3 \pmod 5 = 3$
$3^2 = 9 \pmod 5 = 4$
$3^3 = 27 \pmod 5 = 2$

} all are under GF(5)

Page No.:
Date: / /

1

If 4 is primitive element.

$4^0 = 1 \pmod 3 = 1$
$4^1 = 4 \pmod 3 = 4$
$4^2 = 16 \pmod 5 = 1$
$4^3 = 64 \pmod 5 = 4$

which are not all under GF.
∵ 2, 3 & that.

∴ 4 is not primitive. ⇒ Hy 1 & 5 aren't prim
2, 3 are primitive

GF(7).

Consider, element 2 to be primitive

$2^0 = 1 \pmod 7 = 1$
$2^1 = 2 \pmod 7 = 2$
$2^2 = 4 \pmod 7 = 4$
$2^3 = 8 \pmod 7 = 1$
$2^4 = 16 \pmod 7 = 2$
$2^5 = 32 \pmod 7 = 4$
$2^6 = 64 \pmod 7 = 1$

2 is not primitive

Element 3 is primitive under GF(7)

$3^0 = 1 \pmod 7 = 1$
$3^1 = 3 \quad (\text{—}) = 3$
$3^2 = 9 \quad (\text{—}) = 2$
$3^3 = 27 \quad \text{—} = 6$
$3^4 = 81 \quad \text{—} = 4$
$3^5 = 243 \quad \text{—} = 5$
$3^6 = 729 \quad \text{—} = 1$

all elements are in it except 0.
∴ It is Primitive

Hy, 5 is also primitive.

→ How to find out primitive element?

Prime poly → Irred. (non-factorised) & monic

Properties of PRIMITIVE ELEMENTS :-

→ There can be more than one primitive element in field, but atleast one must be there.

→ Non-zero elements of every GF form cyclic grp

→ GF(q) will include elements of order (q-1). This will be a primitive element

→ Primitive elements are very useful in constructing fields.

SEPT. 26.

PRIMITIVE POLYNOMIAL

Primitive polynomial P(x) over GF(q) is a prime polynomial with property that in extension evaluated modulo P(x), the field element represented by x is a primitive element

eg :- $x^3 + x + 1$ is primitive polynomial where, x is primitive element.

Properties of Primitive Poly. :-

(i) Primitive poly. of every degree exists over GF.

(ii) It can be used to construct an extension field.

eg :- We can construct GF(8) using primitive poly $P(x) = x^3 + x + 1$.

Let primitive element of GF(8) be x or x.

Then, we represent elements of GF(8) by powers of evaluated modulo P(x).

$x^4 \bmod (x^3+x+1)$ ans.

So, we can form :-

Elements of GF(8)

Power of x or α	Elements of GF(8).
x^1 or x^1	x
x^2 or x^2	x^2
x^3 or x^3	$x+1$
x^4 or x^4	x^2+x
x^5 or x^5	x^2+x+1
x^6 or x^6	x^2+1
x^7 or x^7	1

x^3+x+1

GF(16), x^4+x^1+1

Power of x	Element of GF(16)
x^1	x^1
x^2	x^2
x^3	x^3
x^4	$x+1$
x^5	x^2+x
x^6	x^3+x^2
x^7	x^3+x+1
x^8	x^2+1
x^9	x^3+x
x^{10}	x^2+x+1
x^{11}	x^3+x^2+x
x^{12}	x^3+x^2+x+1
x^{13}	x^3+x^2+1
x^{14}	x^3+1
x^{15}	1

x^3+x+1 | x^3+x+1

Page No. :
Date : / /

MINIMAL POLYNOMIAL :-

The smallest degree polynomial with coeff. in the base field GF(q) that has zero in extension field $GF(q^m)$ is called Minimal Polynomial of.

A field is said to extension field of a field if it is a subfield of.

for eg :- R are extension of rational no.
Complex no. are extension of R no.

THM :-

Assume ~~four~~ ~~non zero~~ elements $\beta_1, \beta_2, \beta_3, \ldots \beta_{q-1}$ denote non-zero elements of Galois field GF(q) such that

$$x^{q-1} - 1 = (x-\beta_1)(x-\beta_2) \ldots (x-\beta_{q-1})$$

for eg :- $x^{5-1} - 1 = (x-1)(x-2)(x-3)(x-4)$
$\Rightarrow x^4 - 1 = (x-1)(x-2)(x-3)(x-4)$

} If given elements are (1,2,3,4) under GF(5)

$\Rightarrow x^7 - 1 = (x-1)(x-2)(x-3)(x-4)(x-5)(x-6)(x-7)$ under GF(8)

$x^3+x+1 \overline{)x^4} \; x$

$x^3+x+1 \overline{)x^4+x^3+x^2+x} \; x+1$

$x^3+x+1 \overline{)x^3+x^2+1}$

x^2+x

x^3+x+1

x^2+1

$x^4 - 1$

Primitive Blocklength: Consider, $n = q^m - 1$ (Blocklength)
is said to be primitive blocklength for ~~blo~~ code over GF(q).
A cyclic code over GF(q) of primitive blocklength q is called a Primitive cycle code.

BCH code is defined over GF(q) with blocklength $q^m - 1$ is said to be Primitive BCH code

To find BCH code:-

Minimal polynomial: $x^{q^m} - 1 - 1 = \prod_J (x - \beta_J)$ (multiple)

$x^4 - 1 = (x-1)(x-2)(x-3)(x-4)$ → It is over GF(5)

The smallest degree polynomial with coeff. in base field GF(q) that has zero in extension field $GF(q^m)$ is called minimal polynomial of β_J.

$x^n - 1 = x^{q^m - 1} - 1 = f_1(x) \cdot f_2(x) \cdot \cdots f_{(p)}(x)$

Contd.

→ Encoder
→ Decoder

used for error correctn eg:- we read scratched CD just bcz of RS codes

REED-SOLOMON codes :- RS(n-k)

n

Data	Parity
k	2t

No. of 1's odd
⇒ odd Parity

00*01 | 0/1.

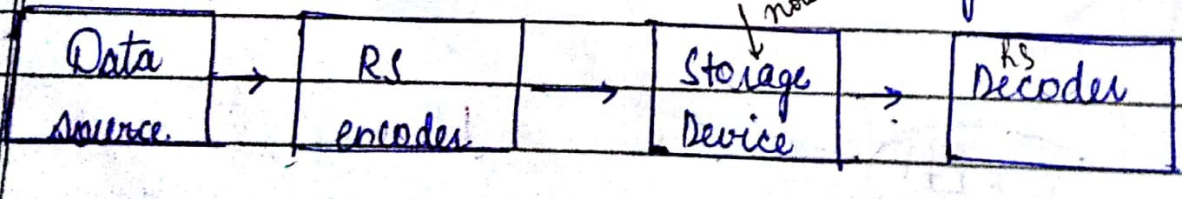
Tx → Rx

} Parity bits are added to get code.

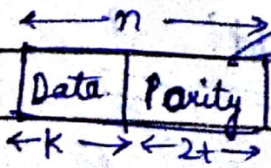
① These are block based error correcting codes with wide range of apps in Digital comm. & storage.
② They are part of BCH & linear codes
③ They are subset of BCH & linear codes.
④ It is specified that RS (n-k)
k → data
n → data + parity

Parity is 2t because codes designed in manner that can correct t errors. In many cases, more than t errors. ∴ $d = 2t+1$

2t → Parity.



encoder :-
↓
Data symbol
↓
(1-bit)



→ Encoder