
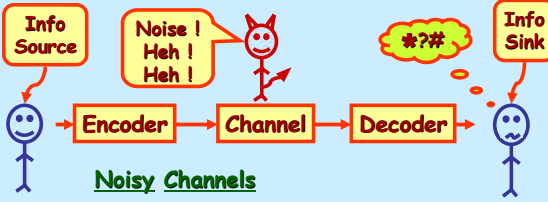


Introduction to Coding Theory

Samuel J. Lomonaco, Jr.
 Dept. of Comp. Sci. & Electrical Engineering
 University of Maryland Baltimore County
 Baltimore, MD 21250
 Email: Lomonaco@UMBC.EDU
 WebPage: <http://www.csee.umbc.edu/~lomonaco>



Why Coding Theory ?



Noisy Channels

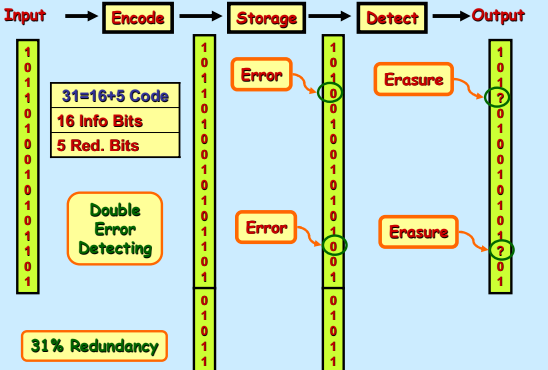
- Computer communication line
- Computer memory
- Space channel
- Telephone communication
- Teacher/student channel

Redundancy

EVN THOUGH LETTERS ARE MISSING FROM THE WORDS IN THIS SENTENCE IT CAN BE RECONSTRUCTED

Error Control Coding

Error Detecting Codes Applied to Memories

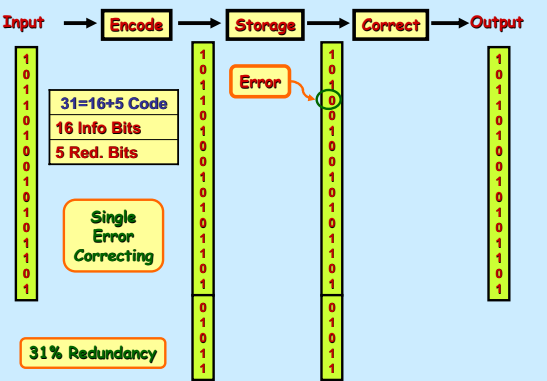


31=16+5 Code
 16 Info Bits
 5 Red. Bits

Double Error Detecting

31% Redundancy

Error Correcting Codes Applied to Memories



31=16+5 Code
 16 Info Bits
 5 Red. Bits

Single Error Correcting

31% Redundancy

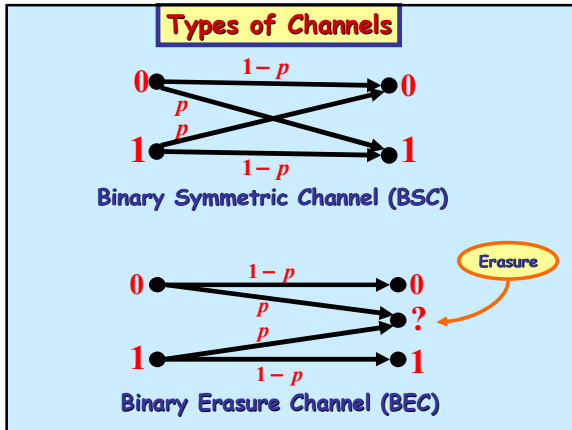
Space Channel

- Mariner Space Probe - Years B.C. (≤ 1964)

E_b/N_0	P_e
6.8 db	10^{-3}
9.8 db	10^{-5}
- Mariner Space Probe - Years A.C.

E_b/N_0	P_e
-1.6 db	Essentially Zero

$1 \text{ db} = \$1,000,000$



2-Repeat Code

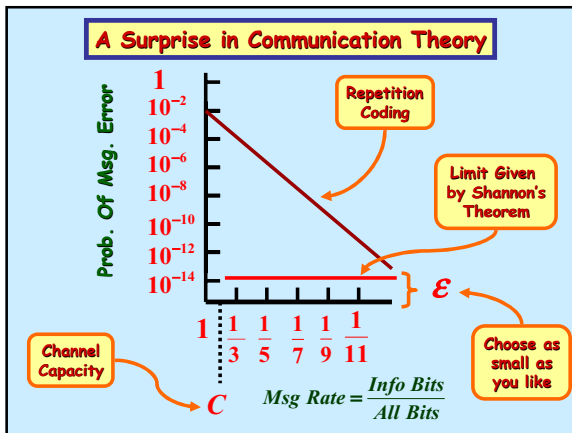
Info. Words	Code Words
0	00
1	11

Detects all single errors

If we use BEC with probability of transition $p = 10^{-2}$, then the probability P_U of undetectable error is

$$P_U = p^2 = 10^{-4}$$

Moreover,

$$Rate = R = \frac{\# \text{ Info Bits}}{\# \text{ All Bits}} = \frac{1}{2}$$


Shannon's Theorem

Within a large class of coding schemes there exist some schemes - nearly all, actually - that give arbitrarily low error rates at any information rate up to a critical rate C , called **channel capacity**.

Folk Theorem

"All codes are good, except those we can think of."

Hamming (8, 4) Code

- Corrects all single errors
- Detects all single, double, and triple errors
- Rate $R = 1/2$

We will now apply this code to the BEC with $p=10^{-2}$

$$P_U < \sum_k C_k^8 p^k (1-p)^{8-k} \approx C_4^8 p^4 (1-p)^4$$

$$\therefore P_U < 70(10^{-2})^4 (1-10^{-2})^4$$

$$\therefore P_U < 6.72 \times 10^{-7}$$

Info Words	Code Words
0000	0000 0000
0001	1101 0001
0010	0111 0010
0011	1010 0011
0100	1011 0100
0101	0110 0101
0110	1100 0110
0111	0001 0111
1000	1110 1000
1001	0011 1001
1010	1001 1010
1011	0100 1011
1100	0101 1100
1101	1000 1101
1110	0010 1110
1111	1111 1111

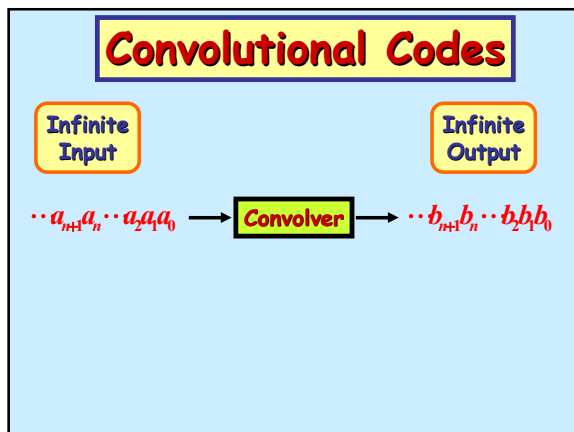
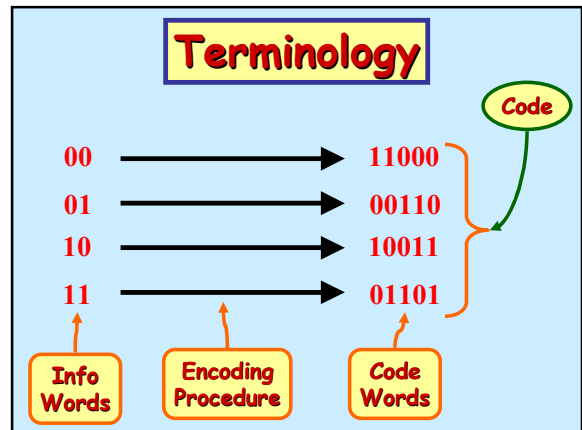
Types of Codes

- A **block code** is a code that uses sequences of n channel symbols, or n -tuples.
 - Only certain selected n -tuples, called **code blocks** or **code words** are sent.
- Convolutional Codes:** Each output bit depends on all the previous bits.

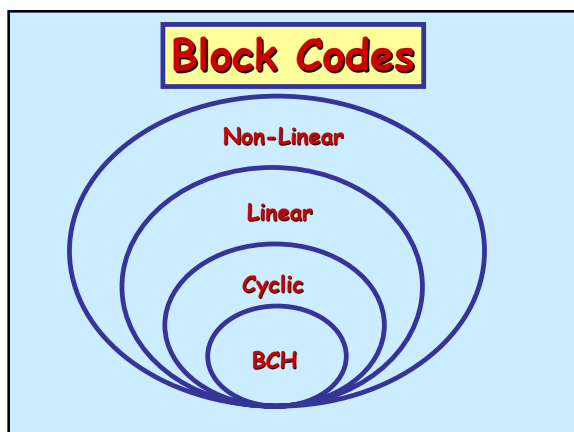
Decoding Table for a Block Code

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

Received Words



- ### Types of Error Correcting Codes
- Block Codes**
- Orthogonal Codes
 - Linear Codes
 - Cyclic Codes
 - BCH Codes
- Convolutional Codes**
- Threshold Decoding
 - Sequential Decoding



Definitions

Def. A **code** is a set of binary vectors of the same fixed length

Parameters of codes

- n = length of code vectors
- R = code rate = (# info bits)/ n
- P_U = Prob. of undetectable error

Problem: P_U depends on the channel

Def. Let u and v be n bit vectors. The **Hamming distance** $H(u,v)$ between u and v is the number of bits at which they differ.

For example,

$$H(0110, 1011) = 3$$

$$H(10011, 00011) = 1$$

Problem: P_U depends on the channel (Cont.)

Def. The **Hamming weight** $H(u)$ of u is the number of 1's in u .

For example,

$$H(0110) = 2$$

Please also note that

$$H(u,v) = H(u+v)$$

Problem: P_U depends on the channel (Cont.)

Def. Let V be a code. Then the **minimum distance** $d(V)$ is

$$d(V) = \text{Min} \left\{ H(u,v) \mid \begin{matrix} u \neq v \\ u, v \in V \end{matrix} \right\}$$

Observation:

$$P_U \leq C_n^d p^d (1-p)^{n-d} + \dots + C_n^n p^n (1-p)^{n-n}$$

So channel independent **Code Parameters** are:

- n = length of code vectors
- R = code rate = (# info bits)/ n
- d = minimum distance

A Recurring Theme

Add More Algebra & Gain

- A trade of space for time, i.e., memory for computation
- Simplifications

Linear Codes

Enter stage right
... Addition

We now adjoin **addition "+"** to the code space

Linear Codes

$GF(2) = \{0,1\}, +, \cdot =$ Galois field of two elts.

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

$E^n = GF(2)^n = \{(b_1, b_2, \dots, b_n) : b_i \in GF(2) \forall i\}$
= n -dim vector space over $GF(2)$

$E^n, +, \cdot$

$$\begin{cases} (b_1, b_2, \dots, b_n) + (b'_1, b'_2, \dots, b'_n) = (b_1 + b'_1, b_2 + b'_2, \dots, b_n + b'_n) \\ a(b_1, b_2, \dots, b_n) = (ab_1, ab_2, \dots, ab_n), a \in GF(2) \end{cases}$$

Linear Codes

Def. A linear code V is a subspace of E , i.e., V is linear iff $u, v \in V \Rightarrow u + v \in V$

Parameters of linear codes:

NOTE:
R=k/n

- n = length of code vectors
- k = $\dim(V) = \log_2(\#V) = \#$ Info. Bits
- d = $d(V)$ = minimum distance

V is said to be a linear (n, k) d code



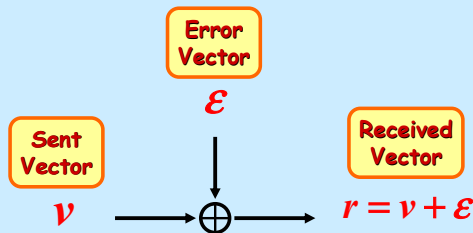
A Simplification

Min. Dist. = Min. Non-Zero Wt.

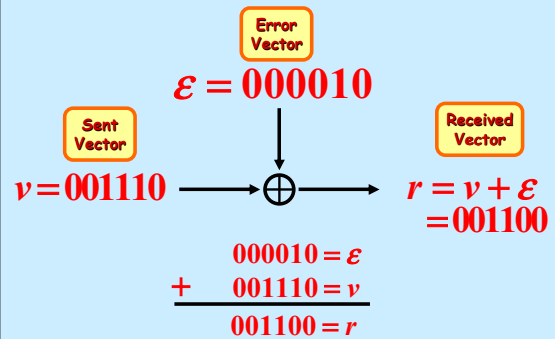
$$d(V) = \text{Min} \left\{ H(u, v) : \begin{array}{l} u, v \in V \\ u \neq v \end{array} \right\}$$

$$= \text{Min} \left\{ H(u) : \begin{array}{l} u \in V \\ u \neq 0 \end{array} \right\}$$

Error Model



An example of the Error Model



An Example: The Hamming (7,4) 3 Code

Infoword \mapsto Codeword

$$(b_3, b_2, b_1, b_0) \mapsto (b_6, b_5, b_4, b_3, b_2, b_1, b_0)$$

where $\begin{cases} b_6 = b_0 + b_2 + b_3 \\ b_5 = b_0 + b_1 + b_2 \\ b_4 = b_1 + b_2 + b_3 \end{cases}$

Infoword	Codeword
0000	000 0000
0001	101 0001
0010	111 0010
0011	010 0011
0100	011 0100
0101	110 0101
0110	100 0110
0111	001 0111

A Linear Code

Infoword	Codeword
1000	110 1000
1001	011 1001
1010	001 1010
1011	100 1011
1100	101 1100
1101	000 1101
1110	010 1110
1111	111 1111

The Hamming (7,4) 3 Code (Cont.)

$$\begin{array}{c} \text{Infoword} \\ (b_3, b_2, b_1, b_0) \end{array} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{array}{c} \text{Codeword} \\ (b_6, b_5, b_4, b_3, b_2, b_1, b_0) \end{array}$$

Generator Matrix G

$$V = \{v \in E^7 : \exists u \in E^4 \text{ s.t. } uG = v\}$$

The rows of G span the linear code V .

A Recurring Theme

Add More Algebra & Gain

- A trade of space for time, i.e., memory for computation
- Simplifications

Cyclic Codes

Enter stage right ... Multiplication

We now adjoin **Multiplication** "•" to the code space

Cyclic Codes: Preliminaries

Each n -bit binary number can be considered to be a polynomial with coefficients over $GF(2)$.

$$10101011 = 1 \cdot x^0 + 0 \cdot x^1 + 1 \cdot x^2 + 0 \cdot x^3 + 1 \cdot x^4 + 0 \cdot x^5 + 1 \cdot x^6 + 1 \cdot x^7$$

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

Cyclic Codes: Preliminaries

1 0 1 1	1 + x ² + x ³
+ 1 1 0 1	+ 1 + x + x ³
0 1 1 0	0 + x + x ² + 0

Addition

Cyclic Codes: Preliminaries

1 0 1	1 + x ²
× 0 1 1	× x + x ²
1 0 1	x + x ³
1 0 1	x ² + x ⁴
0 0 0	x + x ² + x ³ + x ⁴
0 1 1 1 1	

Multiplication

Cyclic Codes: Preliminaries

Problem: Multiplication of code vectors (thought of as polynomials) may increase code vector length.

Example:

$$(101) \cdot (011) = (1 + x^2) \cdot (x + x^2)$$

$$= x + x^2 + x^3 + x^4 = 01111$$

Both Length 3

Length 5

Cyclic Codes: Preliminaries

A quick way to fix the problem:

Assume $x^n=1$ or $x^n+1=0$, where n denotes the codeword length.

Example: $n=3$ Therefore, $x^3=1$

$$\therefore x^4 = x, \therefore x^5 = x^2, \therefore x^6 = x^3 = 1$$

$$\begin{aligned} \therefore 01111 &= x + x^2 + x^3 + x^4 = x + x^2 + 1 + x \\ &= 1 + x + x^2 + x = 1 + (1+1)x + x^2 \\ &= 1 + x^2 = 101 \end{aligned}$$

Cyclic Codes: Preliminaries

Hence, under this identification, the linear space

$$E^n, + = \{(b_0, b_1, \dots, b_{n-1}) : b_i \in GF(2)\}, +$$

becomes a **RING**

$$R_n = \frac{GF(2)[x]}{(1+x^n)}, +, \cdot = \{b_0 + b_1x + \dots + b_{n-1}x^{n-1} : b_i \in GF(2)\}, +, \cdot$$

Cyclic Codes

Def. A linear code V in E^n is a **cyclic code** if

$$(v_0, v_1, \dots, v_{n-1}) \in V \Rightarrow (v_{n-1}, v_0, v_1, \dots, v_{n-2}) \in V$$

Identify $(v_0, v_1, \dots, v_{n-1})$ with the polynomial

$$v(x) = v_0 + v_1x + v_2x^2 + \dots + v_{n-1}x^{n-1}$$

Then a cyclic shift is

$$v(x) \mapsto x \cdot v(x)$$

in the ring $E^n = GF(2)[x]/(1+x^n)$

Cyclic Codes

Proposition. A cyclic code V is an ideal in the ring $GF(2)[x]/(1+x^n)$, i.e.,

$$1) \quad v, v' \in V \Rightarrow v - v' \in V$$

$$2) \quad u \in E^n, v \in V \Rightarrow u \cdot v \in V$$

Generator Polynomial of a Cyclic Code

But E^n is a principal ideal domain. Hence, for every cyclic code V , there exists a polynomial $g(x)$ such that

$$V = (g(x)) = \{u(x)v(x) : u(x) \in E^n\}$$

We choose $g(x)$ so that it is a factor of $1+x^n$. Such a choice is unique.

The polynomial $g(x)$ is called a **generator polynomial** of the cyclic code V .

Generator Polynomial of a Cyclic Code

Proposition. $k = \dim(V) = n - \deg(g)$

Proposition. The generator matrix G of a cyclic code can be written in the form

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}$$

Encoding and Decoding Procedures for Cyclic Codes

Encoding Procedure = Multiplication $g(x)$

$$i(x) \mapsto i(x)g(x)$$

Decoding Procedure = Division by $g(x)$

$$r(x) \mapsto r(x)/g(x)$$

An Example

Consider the cyclic code V given by the generator polynomial $g(x) = 1+x+x^3$

Let n be the smallest positive integer s.t.

$$g(x) \mid (1+x^n)$$

Then $n = 7$ and $\dim(V) = k = n - \deg(g) = 7 - 3 = 4$

This is the Hamming (7,4) 3 code.

If $i(x) = 1+x$, then the encoded vector is

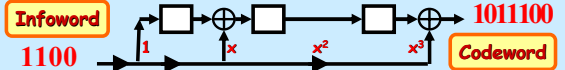
$$(1+x)(1+x+x^3) = 1+x+x^3+x+x^2+x^4 = 1+x^2+x^3+x^4$$

$$\therefore 1100 \mapsto 1011100$$

Another Recurring Theme

Algebra = Computing

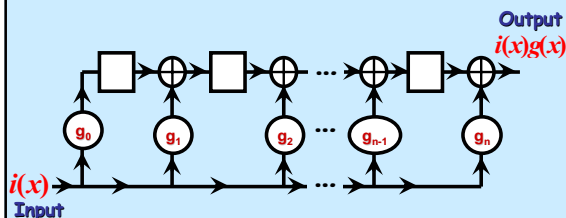
Encoding Circuit = Circuit which Multiplies by $g(x)$



A circuit which multiplies by $1+x+x^3$

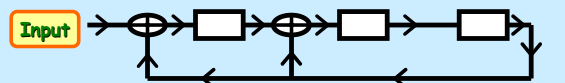
Input	State	Output
1 1 0 0	0 0 0	
1 1 0 0	0 0 0	
1 1 0 0	0 0 0	
1 1 0 0	1 1 0	1 0 0
0 1 0 0	1 1 1	1 1 0 0
0 1 0 0	0 1 0	1 1 0 0
0 0 1 0	0 0 1	1 1 0 0
0 0 0 1	0 0 0	1 1 0 0

General Encoding Circuit which Multiplies by an Arbitrary Generator Polynomial $g(x)$



Linear Circuit for multiplying by $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_{n-1}x^{n-1} + g_nx^n$

Decoding Circuit = Circuit that Divides by $g(x) = 1+x+x^3$

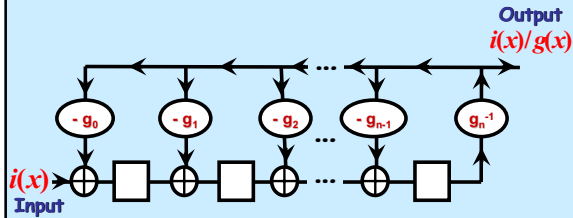


$x^3 g(x) = 0001011000$ ← Initial State

Input	State
0 0 0 1 0 1 1 0 0 0	0 0 0 1 0 1 1 0 0 0
0 0 0 1 0 1 1 0 0 0	0 0 0 1 0 0 1 0 0 1
0 0 0 0 1 0 0 0 1 0	0 0 0 0 1 0 0 0 1 0
0 0 0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 1 0 0
0 0 0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 1 1 0
0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 1 1

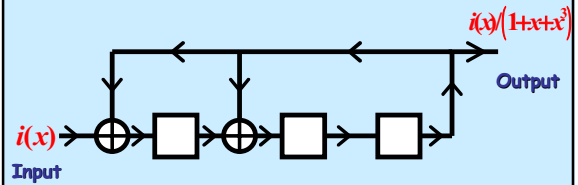
Syndrome
= $S(x) = x+x^2$

General Encoding Circuit which Divides by an Arbitrary Generator Polynomial $g(x)$



Linear Circuit for dividing by $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_{n-1}x^{n-1} + g_nx^n$

An Example



Linear Circuit for dividing by $g(x) = 1 + x + x^3$

A Recurring Theme

Add More Algebra & Gain

- A trade of space for time, i.e., memory for computation
- Simplifications

BCH Codes

Enter stage right
... More Algebraic Structure

BCH = Bose-Chaudhuri-Hocquenghem

Galois Fields (Characteristic 2)

$GF(2^k) = GF[2]/(p(x))$, where

- 1) $\deg(p(x)) = k$
- 2) $p(x)$ is irreducible
- 3) $p(x)$ is primitive, i.e., the residue class ξ containing x generates the multiplicative group of $GF(2^k)$.

Galois Fields (Characteristic 2)

Simplified Approach

$GF(2^k) =$ polynomials in ξ subject to the relation $p(\xi) = 0$.

Example: Construction of $GF(2^3)$

Let $p(x) = 1 + x + x^3$; hence $\xi^3 = 1 + \xi$.

Therefore, every polynomial in ξ reduces to one of the form

$$a_0 + a_1x + a_2x^2,$$

where $a_i \in GF(2)$ for $i = 0, 1, 2$

Example (Cont.)

GF(2³)

0	= 0	= 000
ξ ⁰	= 1	= 100
ξ ¹	= ξ	= 010
ξ ²	= ξ ²	= 001
ξ ⁴	= 1+ξ	= 110
ξ ⁵	= ξ + ξ ²	= 011
ξ ⁶	= 1+ξ+ξ ²	= 111
ξ ⁷	= 1 + ξ ²	= 101

where $a_0 + a_1\xi + a_2\xi^2 \longleftrightarrow a_0 a_1 a_2$

Example (Cont.)

We can create other Galois fields using the following "relations"

GF(2²) with the relation $1+\xi+\xi^2=0$

GF(2³) " " " $1+\xi+\xi^3=0$

GF(2⁴) " " " $1+\xi+\xi^4=0$

GF(2⁵) " " " $1+\xi^2+\xi^5=0$

GF(2⁶) " " " $1+\xi+\xi^6=0$

Another way to describe cyclic linear codes

Another way to describe a cyclic code, i.e., in terms of the roots of the generator polynomial $g(x)$.

$$V = \langle g(x) \rangle = \{ h(x) : h(\alpha) = 0 \text{ for all roots of } g(x) \}$$

Example. Let $V =$ Hamming (7,4) 3 linear code.

Then $g(x) = 1+x+x^3$, and the roots of $g(x)$ are ξ, ξ^2, ξ^4 in $GF(2^3)$. Hence, the linear code is

$$V = \{ h(x) : h(\xi) = h(\xi^2) = h(\xi^4) = 0 \}$$

Moreover, the syndrome is given by

$$r(\xi) = h(\xi) + e(\xi) = e(\xi)$$

BCH Codes

Def. Let ξ be a primitive root of $GF(2^m)$. A cyclic linear code V generated by a polynomial $g(x)$ is a **BCH code with design parameter δ** if $g(x)$ is the polynomial of smallest degree over $GF(2)$ having

$$\xi, \xi^2, \xi^3, \dots, \xi^{\delta-1}$$

as roots.

BCH Codes (Cont.)

If $\delta = 2t_0 + 1$. Then the BCH code can correct t_0 errors, and detect $2t_0$ errors.

Such a BCH code is a cyclic linear $(2^m - 1, k)$ code, where

$$k \geq 2^m - 1 - mt_0$$

$$d \geq \delta$$

An Example

Let ξ be a primitive root of $GF(24)$, where $p(x) = 1+x^3+x^4$

Let V be the cyclic linear code consisting of all vectors $h(x)$ having the roots

$$\xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^{7-1}$$

Then $\xi, \xi^2, \xi^4, \xi^8 \quad m_1(x) = m_2(x) = m_4(x) \quad (\text{deg } 4)$
 $\xi^3, \xi^6, \xi^{12}, \xi^9 \quad m_3(x) = m_6(x) \quad (\text{deg } 4)$
 $\xi^5, \xi^{10} \quad m_5(x) \quad (\text{deg } 2)$

So $g(x) = m_1(x)m_3(x)m_5(x)$; and hence of **deg 10**

Therefore, $(2^{m-1}, k) d = (15, 5) d$, where $d \geq 7$

The End