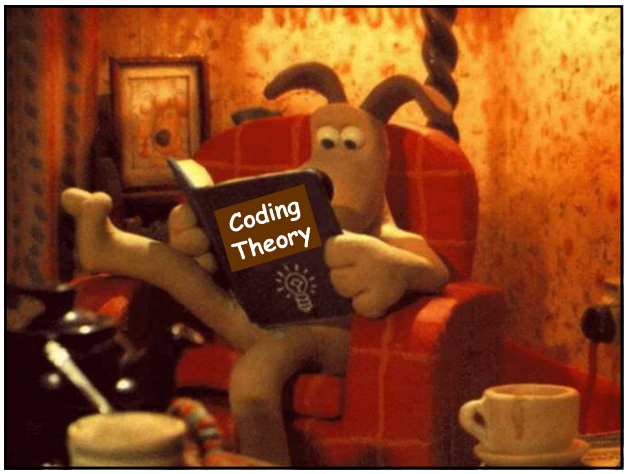
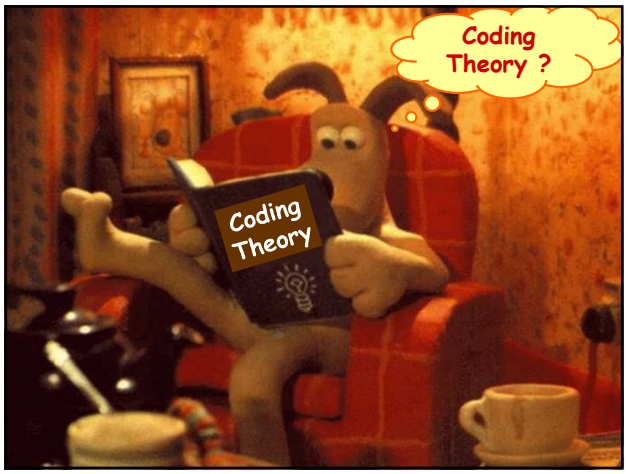


1



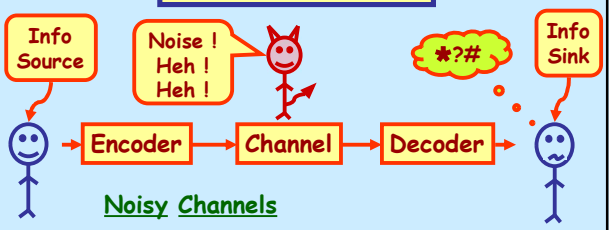
2

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

3

Why Coding Theory ?



Noisy Channels

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

4

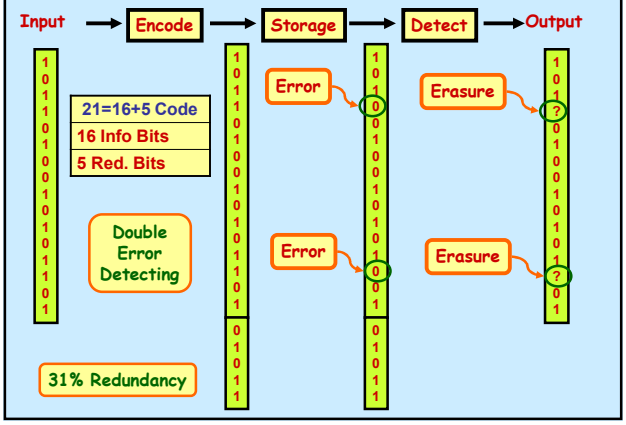
Redundancy

EVN THOUG LTTRS AR MSSNG
FRM TH WRDS N THS SNTNCE
IT CN B NDRSTD

Error Control Coding

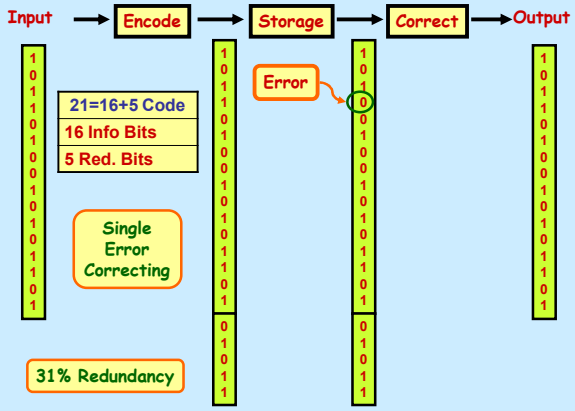
5

Error Detecting Codes Applied to Memories



6

Error Correcting Codes Applied to Memories



7

Space Channel

- Mariner Space Probe – Years B.C. ($\leq$ 1964)

E_b/N_0	P_e
6.8 db	10^{-3}
9.8 db	10^{-5}

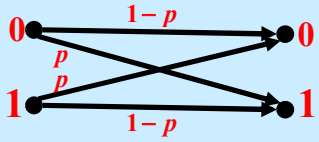
- Mariner Space Probe – Years A.C.

E_b/N_0	P_e
-1.6 db	Essentially Zero

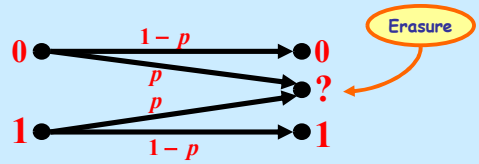
1 db = $1,000,000

8

Types of Channels



Binary Symmetric Channel (BSC)



Binary Erasure Channel (BEC)

9

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

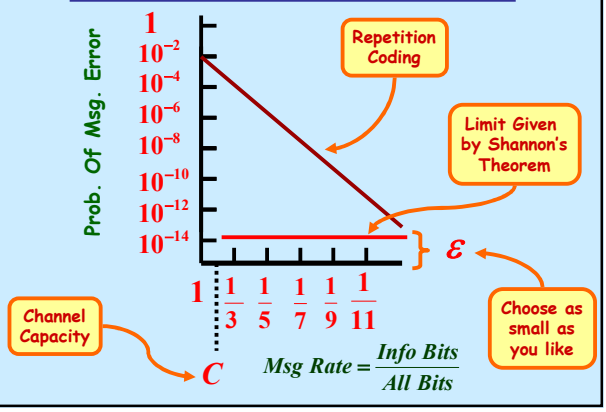
$$P_U = p^2 = 10^{-4}$$

Moreover,

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

10

A Surprise in Communication Theory



11

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."

12

Hamming (8,4) 4 Code

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

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

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

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

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

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

13

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.

14

Decoding Table for a Block Code

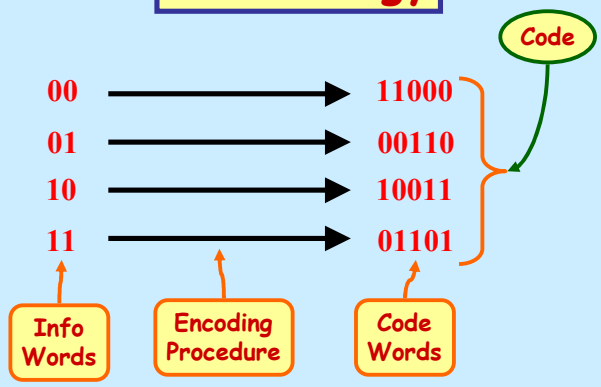
Codewords

Received Words

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

15

Terminology



16

Convolutional Codes

Infinite Input

Infinite Output

$\cdots a_{n+1} a_n \cdots a_2 a_1 a_0 \rightarrow$ Convolver $\rightarrow \cdots b_{n+1} b_n \cdots b_2 b_1 b_0$

17

Types of Error Correcting Codes

Block Codes

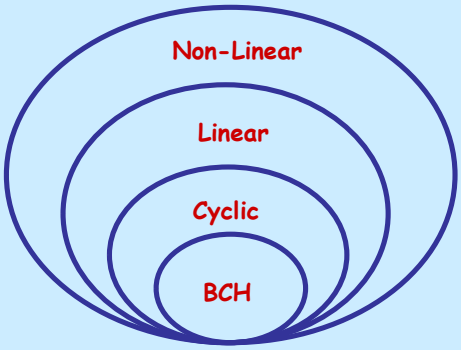
- Orthogonal Codes
- Linear Codes
- Cyclic Codes
- BCH Codes

Convolutional Codes

- Threshold Decoding
- Sequential Decoding

18

Block Codes



19

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

20

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,

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

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

21

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

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

22

Problem: P_U depends on the channel (Cont.)

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

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

Observation:

$$P_U \leq C^n_d p^d (1-p)^{n-d} + \cdots + C^n_n p^n (1-p)^{n-n}$$

So channel independent Code Parameters are:

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

23

A Recurring Theme

Add More Algebra & Gain

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

24

Linear Codes

Enter stage right
... Addition

We now adjoin addition "+" to the code space

25

Linear Codes

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

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

$E^n = GF(2)^n = \{(b_1,b_2,\ldots,b_n) : b_i \in GF(2)\ \forall i\}$

= n-dim vector space over GF(2)

$E^n,+,\bullet$

$$\begin{cases} (b_1,b_2,..,b_n)+(b_1',b_2',..,b_n')=(b_1+b_1',b_2+b_2',..,b_n+b_n') \\ a(b_1,b_2,..,b_n)=(ab_1,ab_2,..,ab_n), a\in GF(2) \end{cases}$$

26

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

Length, Dim, Min. Dist.

27

A Simplification

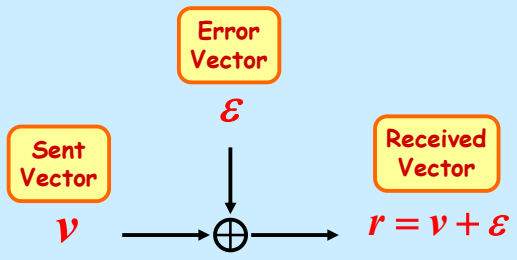
Min. Dist. = Min. Non-Zero Wt.

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

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

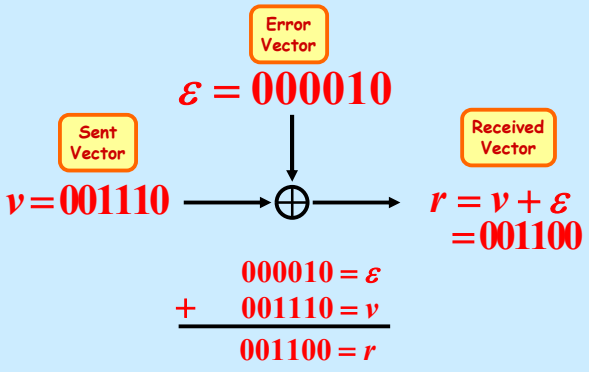
28

Error Model



29

An example of the Error Model



30

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

31

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

Infoword (b_3,b_2,b_1,b_0) Codeword $(b_6,b_5,b_4,b_3,b_2,b_1,b_0)$

$$(b_3,b_2,b_1,b_0)\begin{pmatrix}1&0&1&1&0&0&0\\1&1&1&0&1&0&0\\0&1&1&0&0&1&0\\1&1&1&0&0&0&1\end{pmatrix}=(b_6,b_5,b_4,b_3,b_2,b_1,b_0)$$

Generator Matrix G

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

The rows of G span the linear code V.

32

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

Codeword $(b_6,b_5,b_4,b_3,b_2,b_1,b_0)$

$$(b_6,b_5,b_4,b_3,b_2,b_1,b_0)\begin{pmatrix}1&0&0&1&1&0&1\\0&1&0&0&1&1&1\\0&0&1&1&1&1&0\end{pmatrix}^T=(0,0,0)$$

Parity Check Matrix H^T

$$V=\{v\in E^7 : vH^T=\vec{0}\}$$

The rows of H^T span the linear code $V^\perp$.

33

Linear Codes

- The rows of the generator matrix G span the code V.
- The columns of the parity check matrix H span the dual code $V^\perp$.

34

Linear Codes

Def. Let V be a linear code in E^n. Then the dual code $V^\perp$ of V is

$$V^\perp=\{v\in E^n : v\bullet u=0, \forall u\in V\}$$

where

$$v\bullet u=\sum_i v_i u_i$$

35

Linear Codes

Observation: $v\in V \Leftrightarrow vH^T=0$

Hence, $(v+e)H^T=vH^T+eH^T=eH^T$

Def. Let $\vec{r}$ be a received vector. Then

$$\vec{r}\bullet H^T$$

is called the syndrome of $\vec{r}$.

The syndrome depends only on the error pattern e.

36

Maximum Likelihood Decoding

Coset Leaders
Error Patterns

Code

Decoding Table

000000	001110	010101	100011	011011	101101	110110	11100
000001	001111	010100	100010	011010	101100	110111	111001
000010	001100	010111	100001	011001	101111	110100	111010
000100	001010	010001	100111	011111	101001	110010	111100
001000	000110	011101	101011	010011	100101	111110	110000
010000	011110	000101	110011	001011	111101	100110	101000
100000	101110	110101	000011	111011	001101	010110	011000
001001	000111	011100	101010	010010	100100	111111	110001

Standard Array for a Linear (6,3) 3 Code

37

Maximum Likelihood Decoding

Most Probable Error Pattern for Given Syndrome

Error/Syndrome Table

Error	Syndrome
000000	000
000001	001
000010	010
000100	100
001000	110
010000	101
100000	011
001001	111

38

A Recurring Theme

Add More Algebra & Gain

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

39

Cyclic Codes

Enter stage right … Multiplication

We now adjoin Multiplication "•" to the code space

40

Cyclic Codes: Preliminaries

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

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

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

41

Cyclic Codes: Preliminaries

$$\begin{array}{cccc} 1 & 0 & 1 & 1 \\ + \; 1 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 0 \end{array}$$

$$\begin{array}{ll} 1 & + x^2 + x^3 \\ + \; 1 + x & + x^3 \\ \hline 0 + x + x^2 + 0 & \end{array}$$

Addition

42

Cyclic Codes: Preliminaries

$$\begin{array}{r} 1\ 0\ 1 \\ \times\ 0\ 1\ 1 \\ \hline 1\ 0\ 1 \\ 1\ 0\ 1 \\ 0\ 0\ 0 \\ \hline 0\ 1\ 1\ 1\ 1 \end{array}$$

$$\begin{array}{r} 1 \quad +x^2 \\ \times \quad x+x^2 \\ \hline x \quad +x^3 \\ x^2 \quad +x^4 \\ \hline x+x^2+x^3+x^4 \end{array}$$

Multiplication

43

Cyclic Codes: Preliminaries

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

Example:

$$(101)\bullet(011)=(1+x^2)\bullet(x+x^2)$$
$$=x+x^2+x^3+x^4=01111$$

Both Length 3

Length 5

44

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, $x^3=1$

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

$$\therefore 01111=x+x^2+x^3+x^4=x+x^2+1+x$$
$$=1+x+x^2+x=1+(1+1)x+x^2$$
$$=1+x^2=101$$

45

Cyclic Codes: Preliminaries

Hence, under this identification, the linear space

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

becomes a **RING**

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

46

Cyclic Codes

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

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

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

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

Then a cyclic shift is

$$v(x)\mapsto x\bullet v(x)$$

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

47

Cyclic Codes

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

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

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

48

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.

49

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

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

50

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)

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

51

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

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

$$\therefore 1100 \mapsto 1011100$$

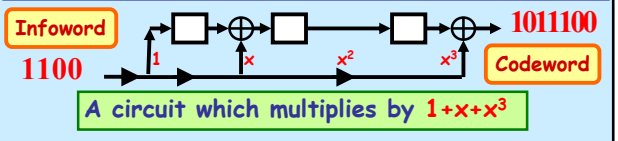
52

Another Recurring Theme

Algebra = Computing

53

Encoding Circuit = Circuit which Multiplies by g(x)

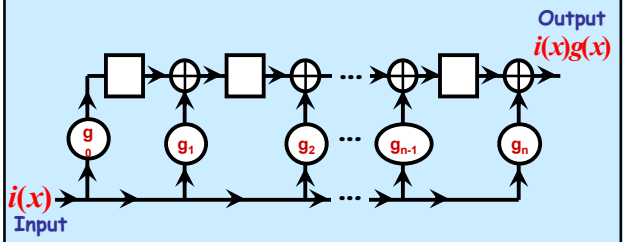


A circuit which multiplies by $1+x+x^3$

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	1	0	1	0	0	
				1	0	1	1	1	0	0
				0	1	0	1	1	1	0
				0	0	1	0	1	1	1
				0	0	0	1	0	1	1

54

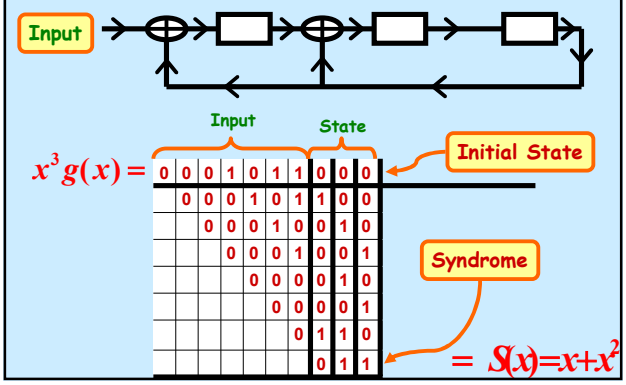
General Encoding Circuit which Multiplies by an Arbitrary Generator Polynomial g(x)



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

55

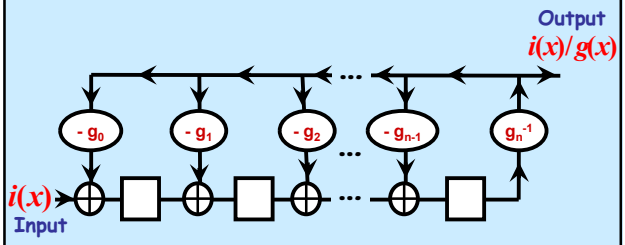
Decoding Circuit = Circuit that Divides by $g(x) = 1+x+x^3$



0	0	0	1	0	1	1	0	0	0
	0	0	0	1	0	1	1	0	0
		0	0	0	1	0	0	1	0
			0	0	0	1	0	0	1
				0	0	0	0	1	0
					0	0	0	0	1
						0	1	1	0
							0	1	1

56

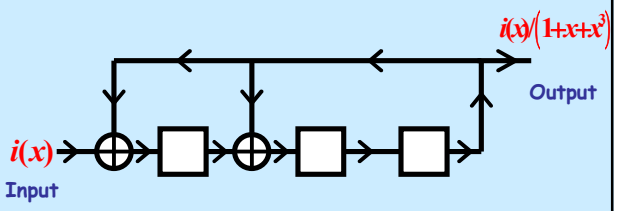
General Encoding Circuit which Divides by an Arbitrary Generator Polynomial g(x)



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

57

An Example



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

58

A Recurring Theme

Add More Algebra & Gain

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

59

BCH Codes

Enter stage right … More Algebraic Structure

BCH = Bose-Chaudhuri-Hocquenghem

60

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 $GF(2^k)$.

61

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 $p(x) = 1+\xi+\xi^3$; 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 e $GF(2)$ for i = 0,1,2

62

Example (Cont.)

$GF(2^3)$

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

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

63

Example (Cont.)

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

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

$GF(2^3)$ " " " $1+\xi+\xi^3 = 0$

$GF(2^4)$ " " " $1+\xi+\xi^4 = 0$

$GF(2^5)$ " " " $1+\xi^2+\xi^5 = 0$

$GF(2^6)$ " " " $1+\xi+\xi^6 = 0$

64

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) .

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

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

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

65

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

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

as roots.

66

BCH Codes (Cont.)

Id $\delta = 2t_0+1$. Then the BCH code can correct t0 errors, and detect 2t0 errors.

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

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

67

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

ξ, ξ^2, ξ^4, ξ^8	$m_1(x)=m_2(x)=m_4(x)$ (deg 4)
$\xi^3, \xi^6, \xi^{12}, \xi^9$	$m_3(x)=m_6(x)$ (deg 4)
ξ^5, ξ^{10}	$m_5(x)$ (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 $d \geq 7$

68

The End

69