CHANNEL CODING

By
Prof. S. J. Soni
Assistant Professor
Computer Engg. Department
SPCE, Visnagar

Overview

From last chapter we can conclude that,

- The key to achieving error-free digital communication in the presence of distortion, noise and interference is the addition of appropriate redundancy to the original data bits.
- The addition of a single parity check digit to detect an odd number of errors is a good example.
- Since shannon's pioneering paper, a great deal of work has been carried out in the area of forward error correcting (FEC) codes.

Overview

- Generally, there are two important classes of FEC codes:
  - Block Codes
  - Convolutional Codes
- *In block codes*, every block of k data digits is encoded into a longer codeword of n digits ($n>k$). Every unique sequence of k data digits fully determine a unique codeword of n digits.
- *In convolutional codes*, the coded sequence of n digits depends not only on the k data digits but also on the previous N-1 data digits ($N>1$). In short, the encoder has memory.

Noise channel Coding Theorem

- It states that for a noisy channel with a capacity C, there exist codes of rate R<C such that maximum likelihood decoding can lead to error probability

$$P_e <= 2^{-n\,Eb(R)}$$

  - where $E_b(R)$ is the energy per information defined as a function of code rate R.
  - This result shows that **arbitrarily small** error probability can be achieved by increasing the block code length *n* while keeping the code rate constant.
  - Thus the key problem in code design is the dual task of searching for good error correction codes with large length n to reduce error probability, as well as decoders that are simple to implement.

Redundancy for Error Correction

- In FEC codes, codeword is a unit of bits that can be decoded independently.
- The number of bits in a codeword is known as the **code length**.
- If k data digits are transmitted by a codeword of n digits, the number of check digits is $m=n-k$.
- The code rate is $R=k/n$.
- Such a codeword is known as an (n, k) code.
- Data digits $(d_1,d_2,\ldots,d_k)$ is a k-dimensional vector d.
- Codeword $(c_1,c_2,\ldots,c_n)$ is an n-dimensional vector c.

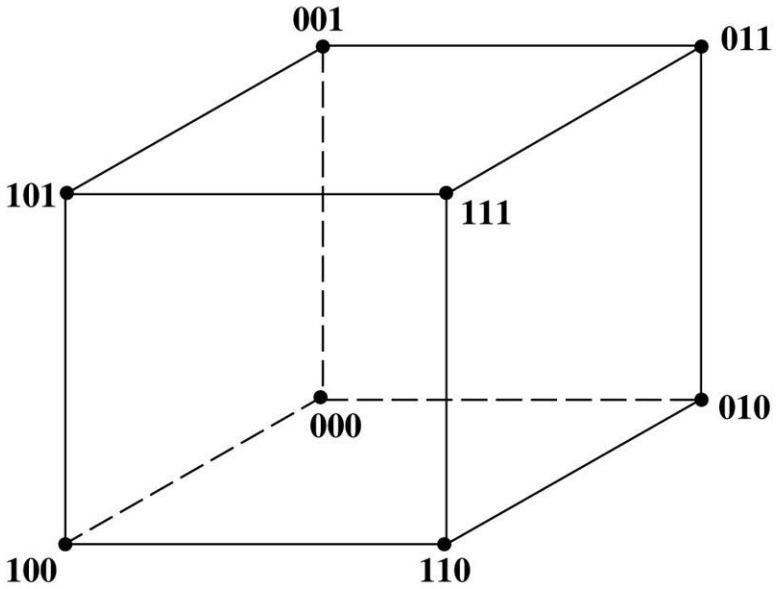
Redundancy for Error Correction

- If the binary code length is n, then the total of 2^n codewords is available to assign to 2^k data words.
- Suppose we wish to find a code that will correct up to t wrong digits. In this case, if we transmit a data word d_i by using one of the code words c_i, then because of channel errors the received word will not be c_i but will be c'_i.
- The minimum distance between t error correcting codewords without overlapping, is

$$d_{min} = 2t + 1$$

Redundancy for Error Correction

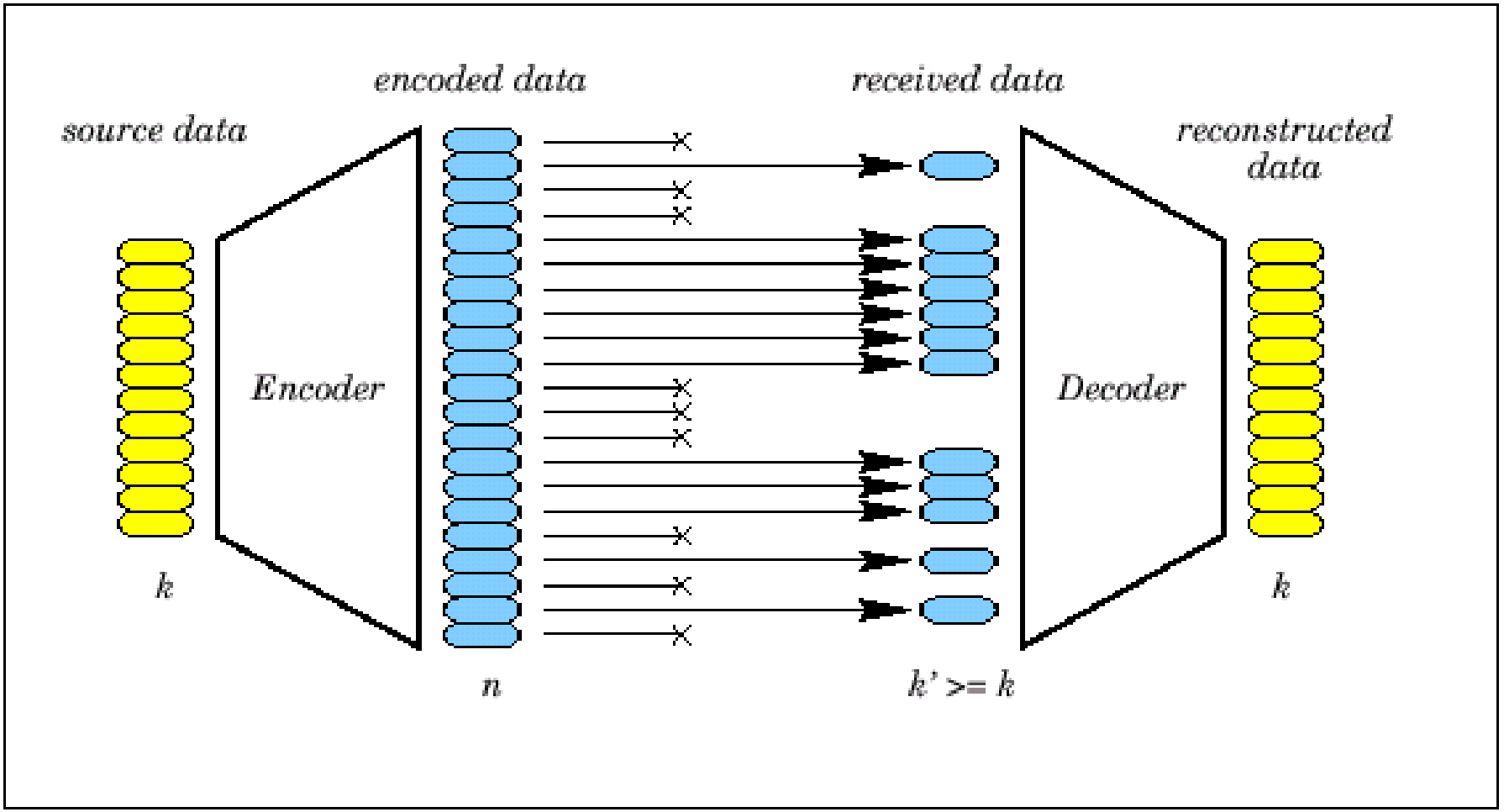
- Consider a simple method of reducing P_e by repeating a given digit an odd number of times. For example, we can transmit 0 and 1 as 000 and 111.
- Here, repetitions cause redundancy but improves P_e.



Three-dimensional cube in Hamming space.

- If two binary sequences of the same length differ in j places, then the ***Hamming Distance*** between the sequences of the same length differ in j places.
- Thus the Hamming Distance between 000 and 010 is 1, and is 3 between 000 and 111.

Error Correction Model



Some examples of Error Correcting Codes

	n	k	Code	Code Efficiency Or Code Rate
Single Error Correcting, t=1 Minimum Code Separation 3 $D_{min} = 2t + 1 = 3$	3	1	(3,1)	0.33
	4	1	(4,1)	0.25
	5	2	(5,2)	0.4
Double Error Correcting, t=2 Minimum Code Separation 5 $D_{min} = 2t + 1 = 5$	10	4	(10,4)	0.4
	15	8	(15,8)	0.533
Triple Error Correcting, t=3 Minimum Code Separation 7 $D_{min} = 2t + 1 = 7$	10	2	(10,2)	0.2
	15	5	(15,5)	0.33

- Hamming Code are (n,k) codes with $n=2^m-1$ and $k= 2^m-1-m$ and minimum distance $d_{min}=m$.
- In general, Hamming Code as $(2^m-1, 2^m-1-m, m)$ code.
- One of the most well-known Hamming Codes is the (7, 4, 3) code.

Linear Block Codes

- Consider codeword $c = (c_1, c_2, \ldots, c_n)$ and data word $d = (d_1, d_2, \ldots, d_k)$
- For general case of linear block codes, all the n digits of c are formed by linear combinations of k data digits.
- A special case in which $c_1=d_1$, $c_2=d_2$,…, $c_k=d_k$ and remaining digits from c_{k+1} to c_n are linear combinations of $d_1, d_2,\ldots, d_k$, is known as a ***systematic code***.
- Here, the leading k digits of a codeword are the data digits and the remaining m=n-k digits are the ***parity check digits***, formed by linear combination of data digits $d_1, d_2,\ldots, d_k$

Linear Block Codes - Example

- For a (6, 3) code the generator matrix G is

$$G = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

I_k P

For all eight possible data words, find the corresponding codewords, and verify that this code is a single error correcting code.

Linear Block Codes - Example

Data Word d	Codeword c
111	111000
110	110110
101	101011
100	100101
011	011101
010	010011
001	001110
000	000000

Linear Block Codes - Example

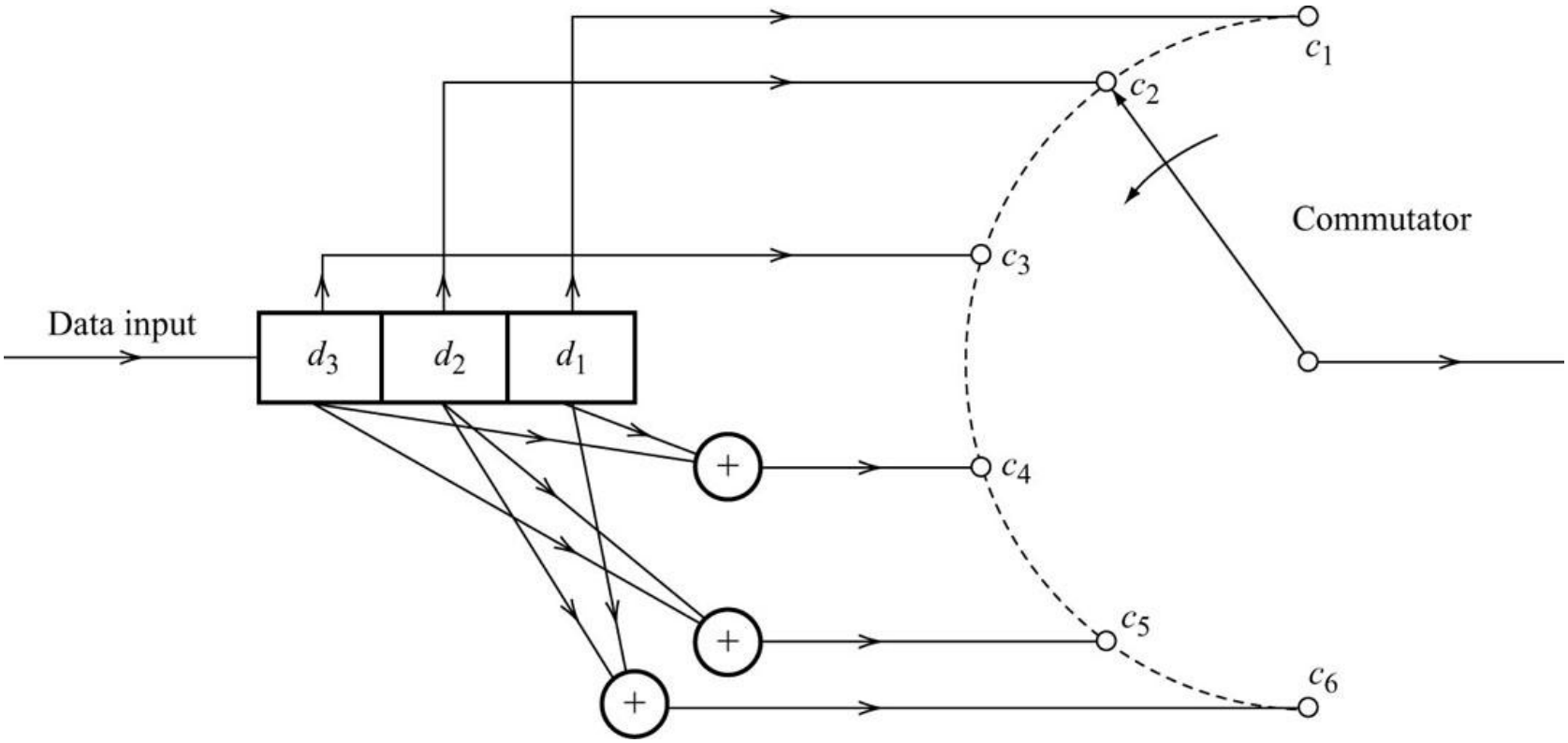
- For a (6, 3) code the generator matrix G is

$$c = [1\ 1\ 1] \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} & & & 1 & 0 & 1 \\ 1\ 1\ 1 & & [1\ 1\ 1] & 0 & 1 & 1 \\ & & & 1 & 1 & 0 \end{pmatrix}$$

$$= 1\ 1\ 1\ 0\ 0\ 0$$

Linear Block Codes - Example



Encoder for linear block codes

Linear Block Codes – Decoding Example

A linear (6,3) code is generated according to the generating matrix in earlier example. The receiver receives r = 100011. Determine the corresponding data word if the channel is a BSC and the maximum likelihood decision is used.

Here, $s = r\,H^T$

$$s = [1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1] \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\mathbf{s = [1\ \ 1\ \ 0]}$$

Linear Block Codes – Decoding Example

- The correct transmitted codeword c is given by

$$c = r \; \textit{ExOR} \; e$$

where e satisfies $s = [1 \;\; 1 \;\; 0] = e\,H^T$

So, $s = [e_1 \;\; e_2 \;\; e_3 \;\; e_4 \;\; e_5 \;\; e_6]$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Linear Block Codes – Decoding Example

- We see that e = 001000 satisfies this equation. But so does e = 000110 or 010101 or 011011 or 111110 or 110000 or 100011.
- The suitable choice, the minimum weight, e_{min}, is 001000. Hence,

c = 100011 exor 001000

= 101011

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Constructing Hamming Codes

- Let us consider a single error correcting code (7, 4)
- In this case m = n-k = 7-4 =3
- There are exactly seven single-error patterns.
- Consider a single error pattern e = 1000000
- Now $s = e H^T$
- Note that H^T is an (n X n-k) matrix. E.g. 7 X 3
- Because there exist seven non-zero patterns of three digits, it is possible to find seven nonzero rows of three digits each. There are many ways in which these rows can be ordered. But we emphasize that three bottom rows must form the identity matrix I_m.

Constructing Hamming Codes

- One possible form of H^T is

$$H^T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} P \\ \\ I_m \end{pmatrix}$$

The corresponding generator matrix G is

$$G = [\, I_k \quad P] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Thus when d = 1011, the corresponding code word c = 1011001 and so forth.

GTU Paper Example

- Consider a (6,3) linear block code with the parity check matrix H given by

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(i) Find the generator matrix G. (ii) Find the code word for the data bit 101.

GTU Paper Example

- For a (7,4) block code generated by [G] below, explain how the error syndrome helps in correcting a single error.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Cyclic Codes

- Cyclic codes are a subclass of linear block codes.
- A procedure for selecting a generator matrix is relatively easy for single-error correcting codes. This procedure, however, cannot carry us very far in constructing higher order error correcting codes.
- Cyclic codes satisfy a nice mathematical structure that permits the design of higher order correcting codes.
- Also, encoding and syndrome calculations can be easily implemented by using simple shift registers.

Cyclic Codes

- If $c = (c_1, c_2, \ldots, c_n)$

  is a code vector of a code C, then $c^{(i)}$ denotes c shifted cyclically i places to the left, that is,

$$c^{(i)} = (c_{i+1}, c_{i+2}, \ldots, c_n, c_1, c_2, \ldots, c_i)$$

- Cyclic codes can be described in a polynomial form. This property is extremely useful in the analysis and implementation of these codes. The code vector c can be expressed as the n-1 degree polynomial

$$c(x) = c_1 x^{n-1} + c_2 x^{n-2} + \ldots + c_n$$

Cyclic Codes

- The coefficients of the polynomial are either 0 or 1, and they obey the following properties:

$0 + 0 = 0$ $\qquad$ $0 \times 0 = 0$

$0 + 1 = 1 + 0 = 0$ $\qquad$ $0 \times 1 = 1 \times 0 = 0$

$1 + 1 = 0$ $\qquad$ $1 \times 1 = 1$

Cyclic Code - Example

- *Find a generator polynomial g(x) for a (7,4) cyclic code, and find code vectors for the following data vectors: 1010, 1111, 0001, and 1000*

In this case, n =7 and n-k = 3 and

$$X^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

Cyclic Code - Example

As there are 3 irreducible factors, there are $2^3 = 8$ cyclic codes. The 8 generator polynomials are:

(i) $1 = 1$

(ii) $x + 1 = x + 1$

(iii) $x^3 + x + 1 = x^3 + x + 1$

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

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

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

(vii) $(x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

(viii) $(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) = x^7 + 1$

Cyclic Code - Example

- For a (7,4) code, the generator polynomial must be of the order n-k = 3. In this case, there are two possible choices for g(x): x^3+x+1 or x^3+x^2+1
- Let us pick up the latter, that is, $g(x) = x^3+x^2+1$ as a possible generator polynomial.
- For d = [1 0 1 0], $d(x)= x^3+x$
- And the code polynomial is c(x)=d(x) g(x)

$$c(x) = (x^3+x)(x^3+x^2+1)$$
$$= x^6 + x^5 + x^3 + x^4 + x^3 + x$$
$$= x^6 + x^5 + x^4 + x$$

hence c = 1 1 1 0 0 1 0

Cyclic Code - Example

- Similarly, codewords for other data words can be found in following table:

d	c
1010	1110010
1111	1001011
0001	0001101
1000	1101000

- Note that, the structure of the codewords. This is not a systematic code.

Systematic Cyclic Codes

- In a systematic code, the first k digits are data bits, and the last m=n-k digits are the parity check bits.
- Systematic codes are a special case of general codes.
- The codeword polynomial c(x) corresponding to the data polynomial d(x) is given by

$$\mathbf{c(x) = x^{n-k}\, d(x) + p(x)}$$

where p(x) is the remainder from dividing x^{n-k} d(x) by g(x).

Systematic Cyclic Codes - Example

- *Construct a systematic (7,4) cyclic code using a generator polynomial.*

we use, $g(x) = x^3+x^2+1$

consider a data vector d = 1010

here, $d(x) = x^3 + x$

and

$x^{n-k}\, d(x) = x^3 (x^3 + x) = x^6 + x^4$

Systematic Cyclic Codes - Example

$X^3 + X^2 + 1$ ← q(x)

$X^3 + X^2 + 1$) $X^6 + X^4$

$X^6 + X^5 + X^3$

$X^5 + X^4 + X^3$

$X^5 + X^4 + X^2$

$X^3 + X^2$

$X^3 + X^2 + 1$

1 ← p(x)

Hence, from equation $c(x) = x^3\, d(x) + p(x) = x^3(x^3+x) + 1$

$= x^6 + x^4 + 1$ so, c = 1010001

Systematic Cyclic Codes - Example

- We construct the entire code table in this manner.

d	c
1111	1111111
1110	1110010
1101	1101000
1100	1100101
1011	1011100
1010	1010001
1001	1001011
1000	1000110
0111	0111001
0110	0110100
0101	0101110
0100	0100011
0011	0011010
0010	0010111
0001	0001101
0000	0000000

Another method to produce a table

- We can use the earlier procedure to compute the codewords corresponding to data words 1000, 0100, 0010, and 0001. These are 1000110, 0100011, 0010111 and 0001101.
- Now recognize that these four codewords are the four rows of G. [c = d.G]
- Hence,

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Cyclic Code Generation

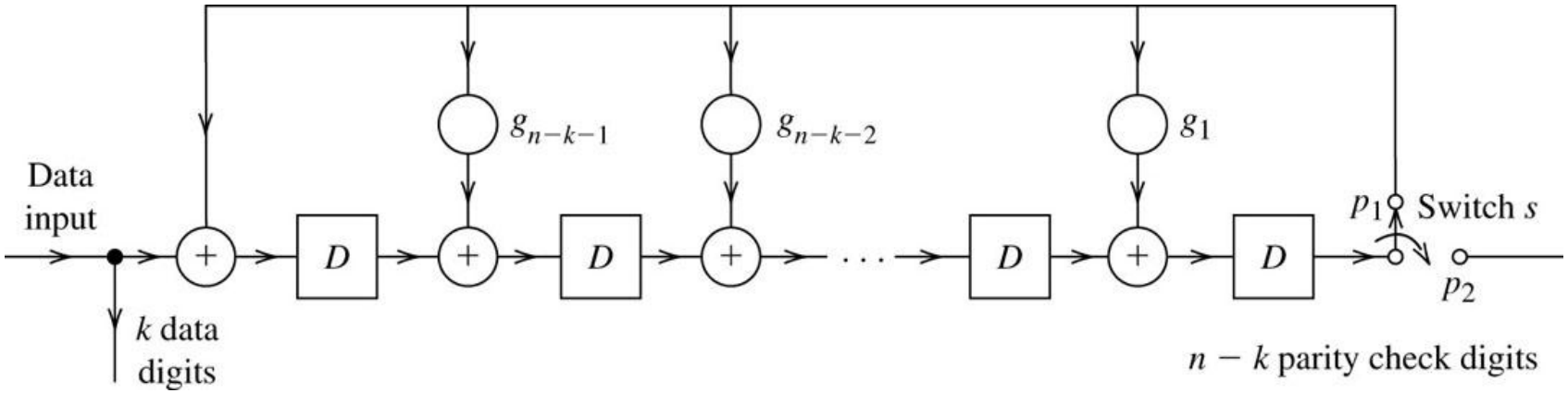


Figure : Encoder for systematic cyclic code.

Decoding of Cyclic Codes

- *Construct the decoding table for the single error correcting (7,4) code. Determine the data vectors transmitted for the following vectors r: (a) 1101101 (b) 0101000 (c) 0001100*

- Here, Because n-k-1 = 2, the syndrome polynomial is of the second order, and there are seven possible nonzero syndromes.
- We use, $s = e \cdot H^T$

Decoding of Cyclic Codes

- To compute the syndrome for each of the seven correctable error patters. Note that,

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$\text{So, } H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Decoding of Cyclic Codes

$$H^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

So, $s = [1\ 0\ 0\ 0\ 0\ 0\ 0] \cdot H^T$

$$s = [1\ 0\ 0\ 0\ 0\ 0\ 0] \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = [1\ 1\ 0]$$

Same way,

e	s
1000000	110
0100000	011
0010000	111
0001000	101
0000100	100
0000010	010
0000001	001

Decoding of Cyclic Codes

- When we received word r is 1101101,

$$s = r \cdot H^T = [1\ 1\ 0\ 1\ 1\ 0\ 1] \cdot H^T = 101$$

- Hence from error syndrome table, this gives

$$e = 0\ 0\ 0\ 1\ 0\ 0\ 0$$

- $c = r$ exOR $e =$ 1101101 exOR 0001000

$$= 1100101$$

Because this code is systematic, d = 1100

GTU Examples

- The generator polynomial of a (7, 4) cyclic code is $g(x) = 1+x+x^3$. Find the code words for the following data (i) 1101 (ii) 0101 (iii) 1001
- Explain coding and decoding techniques for cyclic codes in detail with diagram.
- The generator polynomial for a (15,7) cyclic code is $g(X) = 1+X^4+X^6+X^7+X^8$

  (i) Find the code vector in systematic form for the message $d(X)= X^2+X^3+X^4$

  (ii) Assume that the first and the last bit of the code vector V (X) for $d(x) = X^2+X^3+X^4$ suffers transmission errors. Find the syndrome of V(X)
- Find generator polynomial of a (7, 4) cyclic code with a code word 1110100. Also determine the other code words.

Tutorial Problems

Exercise Problems from B.P. Lathi (Chapter 14)

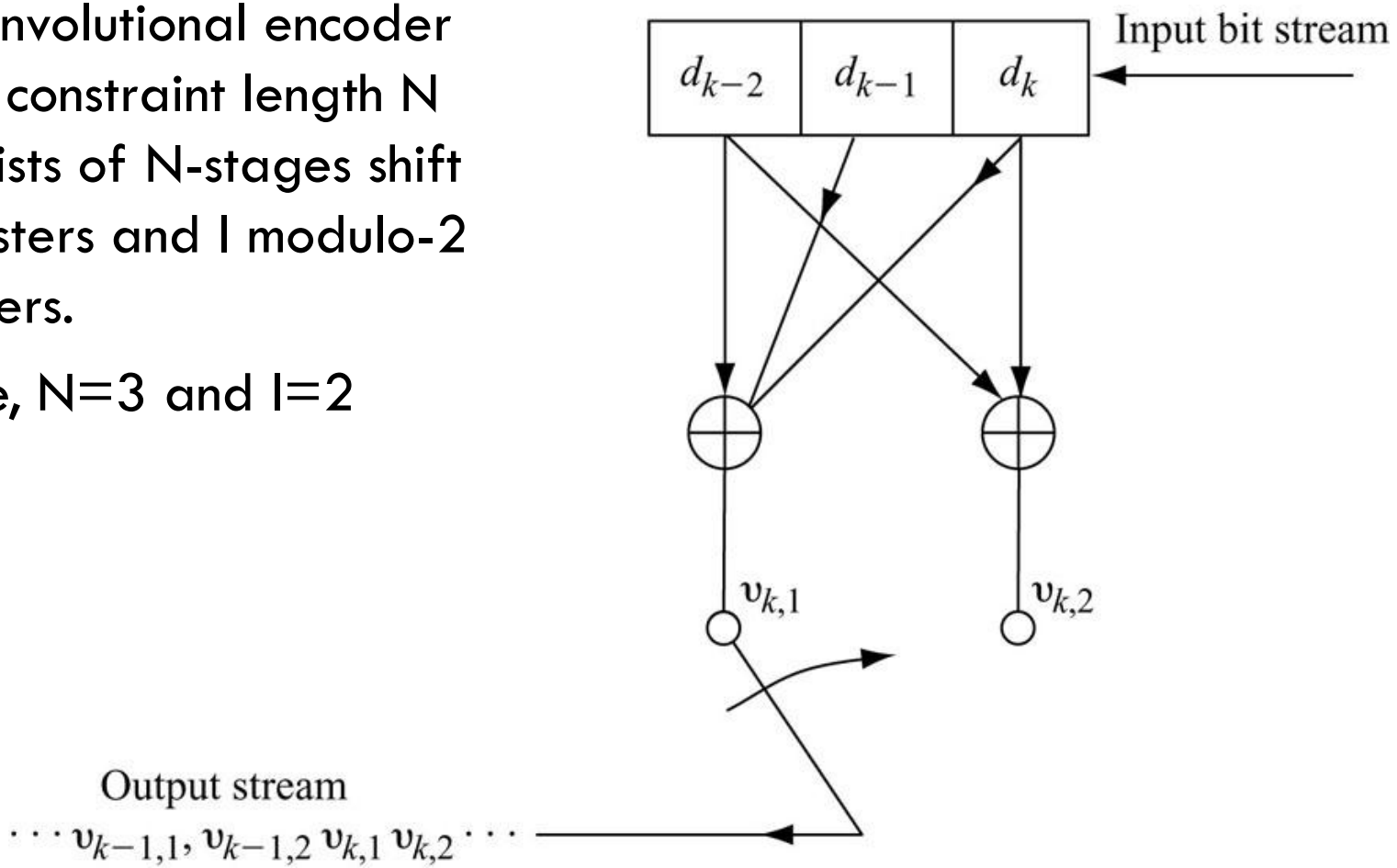
- 14.2-4, 14.2-5, 14.2-6, 14.2-8, 14.2-9, 14.2-14
- 14.3-1, 14.3-2, 14.3-4, 14.3-5, 14.3-6, 14.3-8

Convolutional Codes

- Convolutional (or recurrent) codes are introduced in 1955.
- Here, the block code of n digits generated by the encoder in a particular time unit depends not only on the block of k message digits within that time unit but also on the data digits within a previous span of N-1 time units (N>1), where k and n are usually small.

Convolutional Encoder

- A convolutional encoder with constraint length N consists of N-stages shift registers and I modulo-2 adders.
- Here, N=3 and I=2

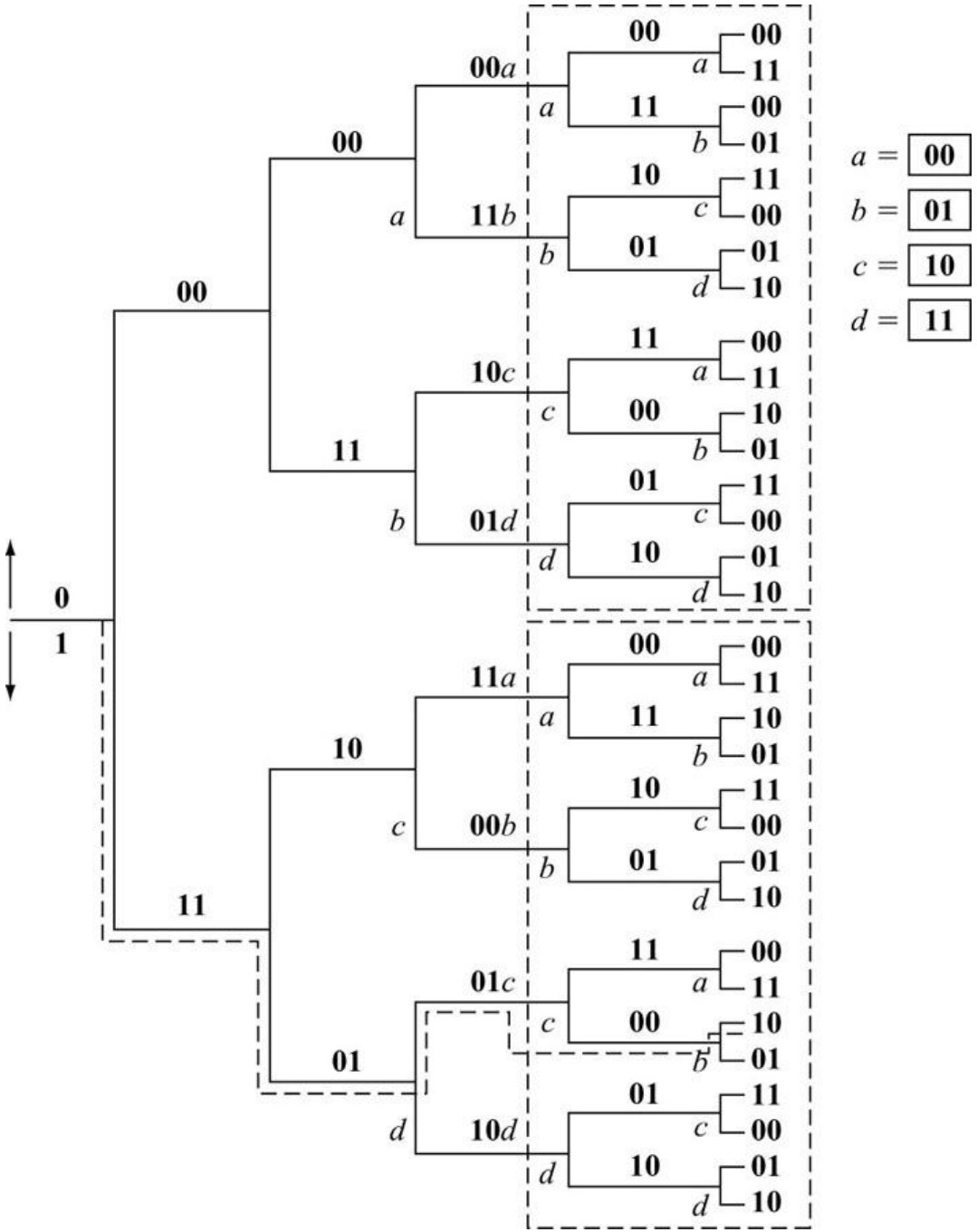


Convolutional Encoder

- *Lets understand operation with reference to the input digits 11010. [N=3 and l=2]*
- Initially, all the contents of the shift registers are 0.

Time k	Dk	Dk-1	Dk-2	Vk,1	Vk,2	Encoder Output
k =1	1	0	0	1	1	11
k=2	1	1	0	0	1	01
k=3	0	1	1	0	1	01
k=4	1	0	1	0	0	00
k=5	0	1	0	1	0	10
k=6	0	0	1	1	1	11
k=7	0	0	0	0	0	00
						11010100101100

Code Tree


0
1
00
11
00
11
10
01
00a
11b
10c
01d
00
11
10
01
00b
01c
10d
a
b
c
d
a = 00
b = 01
c = 10
d = 11

Blog

worldsj.wordpress.com