Error Control Coding

Purpose

To detect and correct error(s) that is introduced during transmission of digital signal.

Introduction

- Error control coding:

  Extra bits(one or more) are added to the data at the transmitter (redundancy) to permit error detection or correction at the receiver.

- Classification of codes:

  1) Error detecting codes: capable of only detecting the errors.

  2) Error correcting codes: capable of detecting as well as correcting the errors.

Classification of Error correcting codes

- Based upon memory:

  Block code: does not need memory.

  Convolutional code: needs memory.

- Based upon linearity:

  Linear code

  Nonlinear code

Types of error control

1. Automatic repeat request(ARQ) technique: receiver can request for the retransmission of the complete or a part of message if it finds some error in the received message. This requires an additional channel called feedback channel to send the receiver’s request for retransmission.

Appropriate for

- Low delay channels
- Channels with a return path

Not appropriate for delay sensitive data, e.g., real time speech and data

2. Forward error correction(FEC) technique: no such feedback path and there is no request is made for retransmission.

- Coding designed so that errors can be corrected at the receiver
- Appropriate for delay sensitive and one-way transmission (e.g., broadcast TV) of data
- Two main types, namely block codes and convolutional codes

Drawbacks of coding techniques

- Higher transmission bandwidth.

- System complexity.

Important definitions

- Code word: The code word is the n bit encoded block of bits. It contains message bits and parity or redundant bits.
- Code rate/code efficiency: It is defined as the ratio of the number of message bits(k) to the total number of bits(n) in a code word.

Code rate (r) = k/n

- Hamming distance: number of locations in which their respective elements differ.

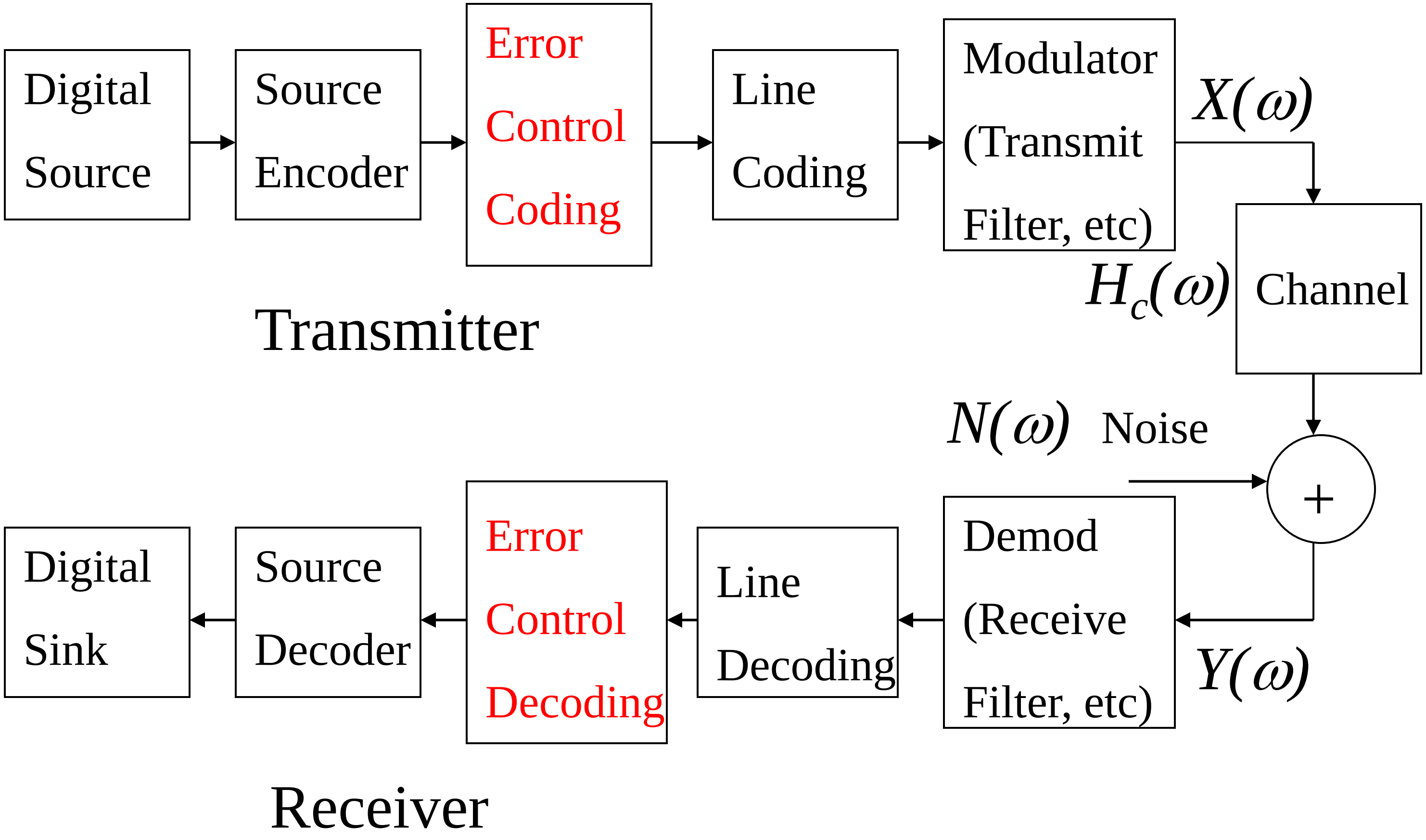
e.g., 10011011

11010010 have a Hamming distance = 3

Alternatively, we can compute by adding code words (mod 2) =01001001 (now count up the ones)

- Hamming weight of a code word: It is defined as the number of nonzero elements in the code word.

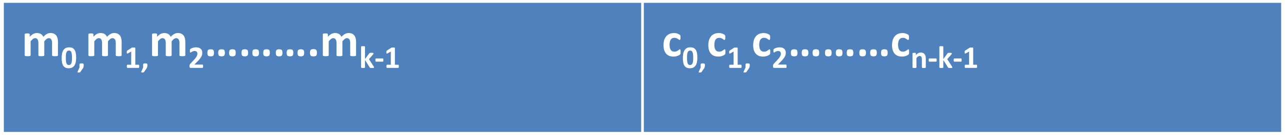
Transmission Model



Linear Block Codes

Definition: A code is said to be linear if any two code words in the code can be added in modulo 2 addition to produce a third code word in the code.

Code word length= n bits

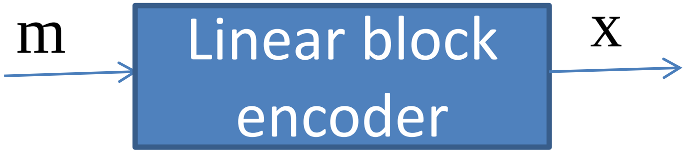


$m_{0,}m_{1,}m_{2}.........m_{k-1}$ $c_{0,}c_{1,}c_{2}........c_{n-k-1}$

k message bits (n-k) parity bits

(n,k) linear block code

- A vector notation is used for the message bits and parity bits
  - message bit m = [$m_0\ m_1....m_{k-1}$]
  - Parity bit c = [$c_0\ c_1........c_{n-k-1}$]



--The code vector can be mathematically represented by

X=[M:C]

M= k message vector

C= (n-k) parity vector

- A block code encoder generates the parity vector or parity bits required to be added to the message bits to generate the code word. The code vector x can also be represented as

$$[X]=[M][G]$$

X=code vector of (1×n) size

M=message vector of (1×k) size

G=generator matrix of (k×n) size

- The generator matrix depends on the type of linear block code used and is defined as

$$G = [\ I_k \mid P]$$

Where I_k = (k×k) identity matrix

P= k×(n-k) coefficient matrix

$$I_k = \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & 1 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{k \times k}$$

$$P = \begin{bmatrix} p_{00} & p_{10} & \cdots & p_{n-k-1,0} \\ p_{01} & p_{11} & \cdots & p_{n-k-1,1} \\ \cdot & \cdot & \cdots & \cdot \\ p_{0,k-1} & p_{1,k-1} & \cdots & p_{n-k-1,k-1} \end{bmatrix}_{k\times(n-k)}$$

- The parity vector can be obtained as

C=MP

$$\begin{bmatrix} c_0 & c_1 \cdots\cdots c_{n-k-1} \end{bmatrix} = \begin{bmatrix} m_0 & m_1 \cdots\cdots m_{k-1} \end{bmatrix} \begin{bmatrix} p_{00} & p_{10} & \cdots & p_{n-k,0} \\ p_{01} & p_{11} & \cdots & p_{n-k,1} \\ . & . & \cdots & . \\ p_{0,n-k} & p_{1,k-1} & \cdots & p_{n-k,k-1} \end{bmatrix}$$

Parity check matrix(H)

- There is another way of expressing the relationship between the message bits and the parity bits of a linear block codes. Let H denote an (n-k)×n matrix defined as

$$H = [P^T \mid I_{n-k}]$$

Where $P^T{}_=$ (n-k)×k matrix representing the transpose of the coefficient matrix P

I_{n-k} = (n-k)×(n-k) identity matrix

Error detection and correction capability of linear block code

- Hamming distance determines the error detecting and correcting capability of a linear block code.

- The maximum number of detectable errors is

$$d_{\min} - 1$$

- The maximum number of correctable errors is given by

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

where $d_{\min}$ is the minimum Hamming distance between 2 code words and $\lfloor \cdot \rfloor$ means the largest integer less than or equal to the enclosed quantity.

Properties of G and H matrix

- $GH^T = 0$
- $HG^T = 0$
- $XH^T = 0$

Example 1,2

Syndrome: Definition & properties

- The generator matrix G is used in the encoding operation at the transmitter. On the other hand, the parity check matrix H is used in the decoding operation at the receiver.

  Let x represent the transmitted code word and y represent the received code word. We express the vector y as the sum of the original code vector X and a vector E, given by

$$Y = X \oplus E$$

  Where E is called the error vector or error pattern. The ith element of the E equals 0 if corresponding element of y is the same as X. On the other hand the ith element of E equals 1 if there is an error at the ith location.

- The syndrome vector is defined as

$$S=YH^T$$

- Property: The syndrome depends only on the error pattern and not on the transmitted code word.

$$S=(X+E)H^T$$

$$=XH^T+EH^T$$

$$= EH^T$$

Syndrome decoding

- We have discussed about the encoder for the linear block code. Now let us learn about the decoder. The two important functions of the decoder are
    - Error detection in the received code
    - Error correction
- The above two functions are accomplished by syndrome decoding.

Detection of Error

- Since we know $XH^T = 0$

  At the receiver, if $S=YH^T = 0$ then $Y=X$ and there is no error but if $S=YHT \neq 0$ then $Y \neq X$ and error exist in the received codeword.

Correction of Error

- Steps:

1. For the given received vector find the syndrome vector as $S=YH^T$.
2. The syndrome vector will resemble any of the column of H matrix, which indicates there is an error in the corresponding bit of the received vector.
3. Now calculate error vector E.

   suppose 2nd column of H matrix and syndrome vector is same that means there is an error at the 2nd bit of received signal. Then the error vector will be E=[0100000] if n=7.
4. Finally determine the transmitted vector as $X = Y \oplus E$

Example 3

Hamming codes

- Consider a family of (n,k) linear block codes that have the following parameters:

Block length: $n=2^m -1$

No. of message bits: $k=2^m -m-1$

No. of parity bits: $n-k=m$

Where $m \geq 3$

These are so called Hamming codes.

- Hamming codes have the property that the minimum distance $d_{\min} = 3$ independent of the value assigned to the no. of parity bits m.

- Thus, Hamming codes are single error correcting code.

Cyclic codes

- Cyclic codes are also linear block codes.
- A binary code is said to be cyclic if it exhibits two fundamental properties:
  - Linearity property: Sum of any two code words in the code is also a code word.
  - Cyclic property: Any cyclic shift of a code word in the code is also a code word.

(n-k) parity bit	**K message bit**

(n,k) cyclic code

Code word polynomial

- The code word [$x_0\, x_1\, x_2$ ….. X_{n-1}] cab be expressed in the form of a code word polynomial as

$$X(p) = x_0 + x_1 p + x_2 p^2 + \ldots\ldots + x_{n-1} p^{n-1}$$

- *Some important conclusion from the code word polynomial:*
  - *For binary codes, the coefficients of p,p2 ………are 1 or 0.*
  - *Each power of p in the polynomial X(p) represents a one bit cyclic shift in time. Thus multiplication of the polynomial X(p) by p is equivalent to a cyclic shift or rotation to right by one digit.*

How do we make such a shift cyclic?

- For this a special type of polynomial multiplication known as modulo (p^n-1) is introduced. Thus a single shift can be obtained by multiplying X(p) by p as

pX(p) mod (p^n-1) = $x_{n-1}+x_0p+x_1p^2+\dots\dots+x_{n-2}p^{n-1}$

The above polynomial represents the code word

$[X_{n-1}\,x_0\,x_1\,x_2\,\dots\dots\,X_{n-2}]$

Generator polynomial for cyclic code

- It is used for the generation of cyclic code words and is represented as

X(p)=M(p)G(p)

Where M(p)=message polynomial

G(p)=generator polynomial of degree (n-k)

$$G(p)=1+g_1 p+g_2 p^2+\dots\dots\dots+g_{n-k-1}p^{n-k-1}+p^{n-k}$$

$$G(p)=1+\sum_{i=1}^{n-k-1} g_i p^i+p^{n-k}$$

NOTE: The degree of generator polynomial is equal to the no of parity bits in the code word.

Cyclic code encoder

- There are three steps involved in the encoding process for an (n,k) cyclic code. They are
  - Multiply the message polynomial M(p) by p^{n-k}
  - Divide $p^{n-k}M(p)$ by the generator polynomial G(p) to obtain the remainder C(p)

$$\frac{p^{n-k}M(p)}{G(p)} = Q(p) \oplus \frac{C(p)}{G(p)}$$

Where Q(p)=Quotient

--Add the remainder polynomial C(p) and $p^{n-k}M(p)$ to obtain the code word polynomial X(p).

i,e, $X(p) = [p^{n-k}M(p)] \oplus C(p)$

Other cyclic codes

- BCH codes
- RS codes

BCH codes

- One of the most important and powerful class of linear block codes.
- Characteristics:
  - Block length: $n=2^m -1$
  - No. of message bits: $k \geq n-mt$
  - Minimum distance: $d_{min} \geq 2t+1$

where $m \geq 3$ and $t = \left\lfloor \frac{2^m - 1}{2} \right\rfloor$

- Each BCH code is a t error correcting code in that it can detect and correct up to t random errors per code word.

Reed-Solomon(RS) Codes

- An important class of non binary BCH code.
- RS code encoder differs from a binary encoder in that it operates on multiple bits rather than individual bits.
- Used in M-ary modulation scheme.
- A t error correcting RS code has he following parameters:
  - Block length: $n=2^m -1$ symbols
  - message size: k symbols
  - Parity check size: $(n-k)=2t$ symbols
  - Minimum distance: $d_{min} = 2t+1$ symbols

Convolutional codes

- In block coding the encoder accepts a k bit message block and generates an n bit code word. Thus code words are produced on a block by block basis. Clearly provision must be made in the encoder to buffer an entire message block.

- In some application message bits come in serially rather than in large block, in which case the use of convolution code is preferred. i,e, They operate on code streams (not in blocks)

- Convolutional codes are applied in applications that require good performance with low implementation complexity.

- Convolution codes have memory that utilizes previous bits to encode or decode following bits (block codes are memory less)

- NOTE: Block codes are more suitable for error detection and the convolutional codes are more suitable for error correction

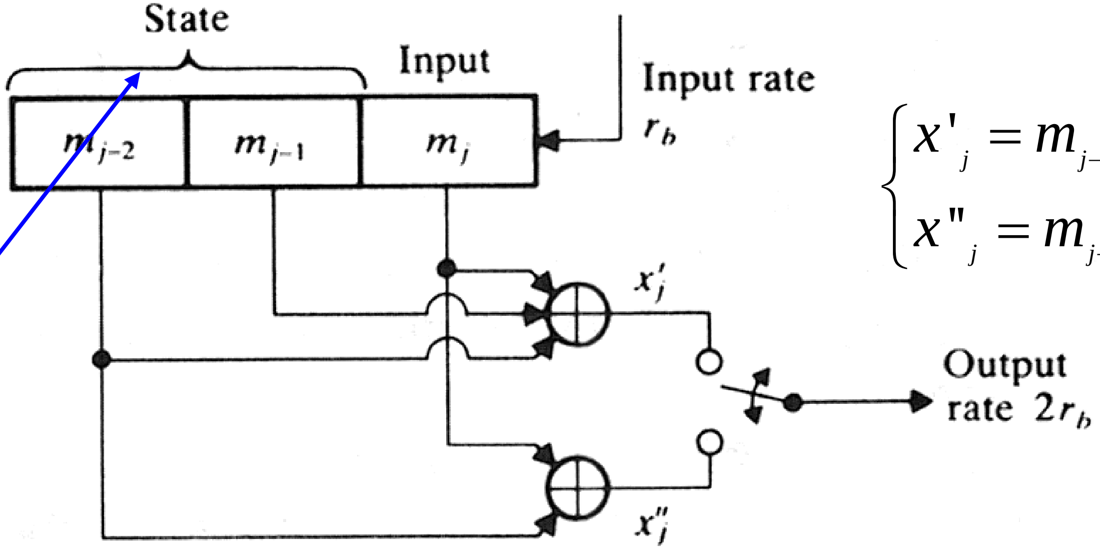
- Representation: A convolutional code is represented as (n,k,L)

Where k=no. of message bits

n= no. of encoded bits

L=encoder’s memory

Example: Convolutional encoder, k = 1, n = 2



$$\begin{cases} x'_j = m_{j-2} \oplus m_{j-1} \oplus m_j \\ x''_j = m_{j-2} \oplus m_j \end{cases}$$

memory
depth *L*
= number
of states

(*n*,*k*,*L*) = (2,1,2) encoder

- Thus, for generation of *n*-bit output, we require in this example *n* shift registers in *k* = 1 convolutional encoder