UNIT-V ERROR CONTROL CODES.

Channel coding theorem

Given a source of M equally likely messages $M \gg 1$, which is generating info at a rate R for a given channel has capacity C then

$$R \leq C \longrightarrow \text{error prob is less.}$$

–ve statement ⟶ $M \gg 1$ generating info at a rate R & channel capacity C then

$$R > C \longrightarrow \text{error prob is close to unity.}$$

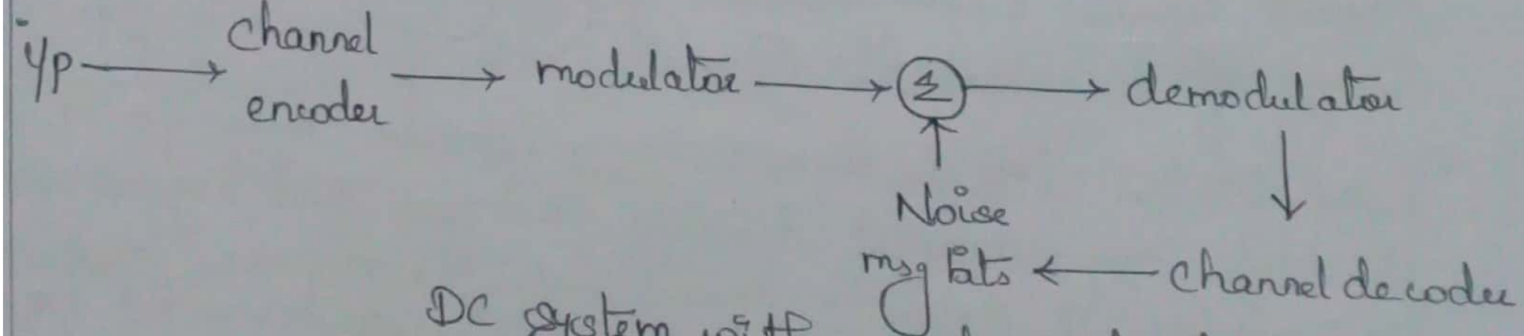
Explain the error detecting

Error Control Coding

⟶ txn of data over the channel depends upon 2 parameters.
- txn power
- channel B/W

⟶ P.S.D of channel noise determines SNR ⟶ determine the error probability of mod scheme.

⟶ Coding tech also reduce SNR for fixed prob of error.



DC system with encoder & decoder.

Error Control Codes
- block codes
- convolutional codes

} Linear / Nonlinear

Block codes → codes consists of n no of bits in one block/ codeword. codeword consists of k msg bits & n-k redundant bits. Block codes → (n, k).

Convolutional Codes → coding operation is discrete time conv of i/p with the impulse response of the encoder. Conv encoder accepts msg bits continuously and generate encoded seq.

Linear → if 2 codes of the linear code are added by mod2 arithmetic it produces 3rd codeword.

Nonlinear → add of nonlinear codeword does not produce 3rd codeword.

Methods of Error Control Coding
- Forward error correction
- error detection with re-transmission.

Forward error correction → errors are detected/corrected by proper coding technique. Check bits/redundant bits are used to detect/correct errors. Error detection capability of rx depends upon the no of redundant bits. Overall prob of error is high.

Error detection with re-transmission → decoder checks i/p seq. When it detects any error, it discards that part and request for re-transmission of data. Tx again sends the msg seq in which error was detected. Note: decoder does not correct errors just request to retransmit seq. Overall prob of error is low.

Error types
- Random Error
- Burst Error

Random Errors → due to white gaussian noise in the channel. errors generated in a particular interval does not affect the system performance. Errors are totally uncorrelated.

Burst Errors → due to impulsive noise in the channel. generated due to lighting & switching char. errors are dependent on each other in successive msg intervals.

Terminology.

(1) Code Word → encoded block of n bits called codewords. Consist of msg bits & redundant bits.

(2) Block length → no of n bits after coding called block length of the code.

(3) Code rate → ratio of msg bits (k) to the encoded o/p bits (n) called code rate $r = k/n$ $0<r<1$.

(4) Channel data rate → bit rate at the o/p of encoder.

$R_0 = n/k\ R_s$.
R_s → i/p of the encoder

(5) Code Vectors → n bit code word visualized in N-dim space.

(6) Hamming distance → distance b/w 2 code vectors is equal to no of elements in which they differ 'd'

1001
1101
d = 2

(7) Min distance (d_{min}) → smallest hamming distance

$d_{min} \leq n-k+1$

(8) Code efficiency → ratio of msg bits in a block to the txn bits

Code efficiency $= k/n$.

(9) Weight of the code → no of non zero elements called weight of the code $W(x)$. $X = 1011 \rightarrow W(x) = 3$.

(10) Free distance → min distance b/w the code vectors that equals to min weight of the code vector.

$$d_f = [w(x)]_{min} \quad x \neq 0.$$

(11) No of errors → $d_f > 2f$

(12) Coding gain → $A = r d_f / 2$

d_f → free distance.

r → code rate

(13) Vector space → set of all code vector called vector space. 3 bit code word $2^3 = 8$ code vectors.

(14) Vector subspace → subset of code vectors of n bit codewords called vector space (subspace).

Linear Block Codes.

Principle → For the block of k msg bits, (n−k) parity bits are added. total bits at the o/p be n. block codes (n, k).

Systematic Codes → msg bits appear at the begining of the code word. msg bits appear first & then check bits are transmitted in a block.

Non systematic code → not possible to identify msg bits they are mixed in nature.

Linear Code → linear if the sum of any 2 code vectors produces another code vector.

$$X = m_1 m_2 \dots m_k, c_1 c_2 \dots c_q$$

$q = n - k$ → no of redundant bits

$X = (M \mid C)$

C → q check bits

M → k msg bits

Matrix.

Code vector $X = MG$

$$[X]_{1\times n} = [M]_{1\times k}[G]_{k\times n}$$

$$[G] = [I_k \mid P_{k\times q}]_{k\times n}$$

Check vector $C = MP$

$$(c_1\ c_2 \dots c_q) = (m_1\ m_2 \dots m_k)_{1\times k}\begin{bmatrix} P_{11} & \dots & P_{1q} \\ P_{21} & \dots & P_{2q} \\ P_{k1} & \dots & P_{kq} \end{bmatrix}$$

$$c_1 = m_1 P_{11} \oplus m_2 P_{21} \oplus \dots \oplus m_k P_{k1}$$

$$c_2 = m_1 P_{21} \oplus m_2 P_{22} \oplus \dots \oplus m_k P_{k2}$$

and so on.

Hamming Codes.

(n, k) linear block codes.

Cond no of check bits $q \geq 3$

Block length $n = 2^q - 1$

msg bits $k = n - q$

min distance $d_{min} = 3$

Code rate $r = k/n$

$$= n-q/n$$

$$= 1 - q/n$$

$n = 2^q - 1$ then $r = 1 - \frac{q}{2^q - 1}$

$r = 1$ if $q >> 1$.

$$GH^T = \left[I_{k \times k} \mid P_{k \times q} \right] \frac{P_{k \times q}}{I_{q \times q}} = P \oplus P = 0$$

Error detection $d_{min} \geq 2+1$ i.e. $d_{min} \geq 3$

Error correction $d_{min} \geq 2+1$ i.e. $d_{min} \geq 3$.

Theorem 1

→ min distance of the linear block code is equal to min weight of any non-zero codeword in code.

Theorem 2

→ linear block code having the min distance of d_{min} can detect upto $d_{min} - 1$ errors & correct upto $d_{min} - 1/2$ errors in each codeword.

Syndrome Decoding.

Generator matrix G used in the encoding operation at the Tx, parity check matrix H.

$X = Y \longrightarrow$ no error

$X \pm Y \longrightarrow$ error during txn

$Y = X + e \longrightarrow$ rx msg.

For eg:

$X = [101011]$

$Y = [111001]$

$e = [010010]$

Rx has the task of decoding the code vector X from the rx vector Y commonly to perform this decoding operation starts with the computation of $1 \times q$ vector called syndrome.

$$S = YH^T$$

Properties.

① Syndrome depends only on the error pattern and not on the tx codeword.

② All error patterns that differ at most by a codeword have the same syndrome.

③ Syndrome S is the sum of those columns of the matrix H corresponding to the error locations.

④ With syndrome decoding (n, k) linear block code can correct upto 't' errors per codeword, that should satisfy $\binom{n}{i} = \frac{n!}{(n-i)!\, i!}$

Cyclic ~~Hamming~~ Codes.

→ Subclass of linear block codes.

→ Easy to encode

Binary code is said to be a cyclic code if every cyclic shift of the codeword or sum of two codewords produce some other codeword.

① Linearity Property → sum of 2 codewords is also a codeword.

② Cyclic Property → any cyclic shift of a codeword is also a codeword.

Representation $x(D) = x_0 + x_1 D^1 + x_2 D^2 + \dots + x_{n-1} D^{n-1}$

2 forms — systematic
— non-systematic

Generator Polynomial.

(n, k) cyclic codes is specified by the complete set of code word polynomials of degree (n-1) with min degree (n-k) as a factor.

degree of $g(D)$ ~~code~~ is equal to no of parity bits.

Properties.

1. Gen polynomial of an (n, k) cyclic code is unique, ie the only codeword polynomial of min degree (n-k).
2. Any multiple of the generator polynomial $g(D)$ is a codeword polynomial a
$$x(D) = a(D)\, g(D) \text{ Mod}(D^{n-1}).$$
3. Gen polynomial $g(D)$ & parity check polynomial $h(D)$ are factors of the polynomial $1+D^n$ is given by
$$h(D)\, g(D) = 1 + D^n.$$

Classes of cyclic codes.

→ CRC
→ BCH
→ Convolutional
→ Viterbi
→ ~~Code Tree & State diagram~~ Golay Codes.
→ RS codes

Cyclic Codes Redundancy.

Cyclic codes for error detection is called CRC. A CRC error burst of length B in an n bit rx word as a contigious seq of B in which the first & last bits and any no of intermediate bits rx are error.

CRC 12 code $\longrightarrow 1 + D + D^2 + D^3 + D^{11} + D^{12}$

16 code $\longrightarrow 1 + D^2 + D^{15} + D^{16}$

char length $\longrightarrow$ 6 bits

char length $\longrightarrow$ 8 bits.

Block length $n = 2^m - 1$

msg bits $k = m$

min distance $d_{min} = 2^m - 1$

$$g(D) = 1 + D^n / h(D) \longrightarrow \text{max length codes.}$$

Golay Codes.

Special case of binary code capable of correcting any combination of rand errors of block 23 bits. Perfect cyclic code has min dist of 7.

Golay code $\longrightarrow (23, 12)$

$$g_1(D) = 1 + D^2 + D^4 + D^5 + D^6 + D^{10} + D^{11}$$

$$g_2(D) = 1 + D + D^5 + D^6 + D^7 + D^9 + D^{11}$$

$$1 + D^{23} = (1 + D)\, g_1(D)\, g_2(D).$$

Disadv $\longrightarrow$ does not generalize.

BCH codes

Cyclic code with wide variety of parameters. +ve m there exists a cond.

block length $n = 2^m - 1$

no of msg bits $k \geq n - mt$

min distance $d_{min} \geq 2t + 1$

RS codes.

Subclass of non-binary BCH codes.

block length $n = 2^m - 1$

msg bits k

parity check bits $n - k = 2t$

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

Adv.

→ highly efficient
→ adjustable
→ provide wide range of code rates.

Convolutional codes.

accepts k msg block & generates n bit codeword. they are produced on block by block range. Encoder must buffer an entire msg block before generating associated codeword.

Operates on the incoming msg sequence in a serial manner. Encoder with the rate of $1/n$ measured in bps.

code rate $r = L/n(L+M)$ bits/symbol

$L >> M$

ie $r = 1/n = k/n$

Viterbi decoding.

Max likelihood decoder that is optimum for white gaussian noise channel for L bit msg seq & encoder of M.

Metric
↳ hamming distance b/w the coded seq represented by the path & rx seq.

Surviving path
↳ path of the decoded signal with min metric

Step 1 → compute metric of the signal path

2 → increment j by 1. for each stage identify the lowest metric

3 → if $j < L+M$ repeat 2 otherwise stop.

$M = k-1$.
↳ constraint length.

Adv.

→ decoding delay is small
→ H/w req is low
→ sync not affect the system performance

Disadv.

→ Complex
→ Codes are not developed.