B B2
IT

Devansh Shah
1914078

21/05/21

ITC ESE

1) b
2) b
3) b
4) a
5) b
6) c
7) a
8) b
9) c
10) a

Devansh
1914078
Delhi (2)

Q1) (B)

3) Run length encoding :- (RLE)

- RLE is a simple form of lossless data compression that runs on sequences with same value of occuring consecutive time.
- It encodes the sequence to store only a single value and it count.

eg) A A A A A A B B C C C C C C D D D D

→ (6, A), (2, B), (6, C), (4, D)

(4)

Devansh
1914078
Dsheh

Q1) (B)

1) Hamming weight

- The hamming weight of a string is the number of symbols that are different from the zero symbol of the alphabet used.
- It is equal to the hamming distance from all zero string of the same length. For most cases this is the number of 1's in the string or the digit sum of the binary representation of given number and the l_4 form of a bit vector.

eg) string - 11101
H.W. - 4

Hamming distance

- The hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different
- It measures the minimum number of substitutions required to change one string into other, or the minimum number of errors that could have transformed one string to other

eg) strings : 0100 → 1001
H.D. : 3

Devansh
1914078
Rishab (4)

4) Types of errors in digital communication systems are caused by the noise present in the communication channel. The two kinds of noise are encountered in communication channel namely gaussian noise and impulse noise.
The types are:-
1) Random error
2) Burst error

→ Burst error
- Impulse noise is characterized by long quite intervals ~~of~~ followed by high amplitude noise burst such as noise arising due to lightning switching transients, man made noise etc.
- When such noise burst occur, the affect more than one symbol and the error caused is called burst error.

eg) sent Received
10 11 00 11 ⇒ 11 00 0 11

6)

Symmetric Cryptography	Asymmetric Cryptography
- It is also called as private key cryptography or secret key cryptography.	It is also called as public key cryptography.
- Only one key is used for encryption and decryption	Two different keys are used - public and private key.
- Symmetric key algorithm are faster in execution.	They are slower in execution.
- less complex and less computational power required.	More complex and more computational power required.
- used to transfer bulk data	Used for securely exchanging the secret key.
- the key is shared between sender and receiver which is not safe.	No problem of key sharing because of private key concept
- Commonly used algorithms DES, AES	Commonly used algorithms RSA, DSA

Devansh
19114078
~~Dsharma~~ (6)

7) Consider that 'p' is an odd prime number and 'a' is an integer such that

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

The congruence $x^2 \equiv a \pmod{p}$ has a soln if & only if $a^{(p-1)/2} \equiv 1 \pmod{p}$

legendary and Jacobi symbols give a simple method to determine whether or not 'a number is square mod p'

⇒ legendary symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \text{ [p divides a]} \\ +1 & \text{if } x^2 \equiv a \pmod{p} \text{ [a is quadratic residue and has a soln mod p]} \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ [a is a quadratic non residue (has no soln mod p]} \end{cases}$$

⇒ Jacobi symbol is defined based on legendary symbol where 'n' is an odd positive composite integer (instead of p) and 'a' is a non zero integer such that gcd (a, n) = 1

Let the prime factor of n are :-

$n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots p_r^{b_r}$ that we have

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{b_1} \cdot \left(\frac{a}{p_2}\right)^{b_2} \cdots \left(\frac{a}{p_r}\right)^{b_r}$$

Devansh
1914078
Dabas

where $\left(\frac{a}{n}\right)$ is jacobi symbol and $\left(\frac{a}{p_i}\right)$ are legendary symbol.

Devansh
1914078
Delhi

(8)

Q2) $G =$

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

i) To find all possible code words,
we know, $C = iG$
So we have all the values of i as this is (6, 3) generator matrix
$k = 3$
All i of length 3 are :-
info words ⇒ 000, 001, 010, 011, 100, 101, 110, 111

To get all code words, multiply i with G

$$C_1 = i_1 G = 000 \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = 000000$$

$C_2 = i_2 G = 001 \times G = 101001$
$C_3 = 010 \times G = 011010$
$C_4 = 011 \times G = 110011$
$C_5 = 100 \times G = 110100$
$C_6 = 101 \times G = 011101$
$C_7 = 110 \times G = 101110$
$C_8 = 111 \times G = 000111$

Devansh
1914078
Dshah (9)

ii) Encoding table

Message	Code word	Weight
000	000000	0
001	101001	3
010	011010	3
011	110011	4
100	110100	3
101	011101	4
110	101110	4
111	000111	3

We have $d_{min} = 3$

$e = d_{min} - 1 = 2$

$t \leq \left[\frac{1}{2} (d_{min} - 1) \right]$

Hence (6, 3) linear block code can detect 2 bit errors and correct 1 bit error in 6 bit o/p code word.

iii) received C.W. = 110101

H parity check matrix can be got from generator matrix

$$P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \qquad P^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$I_{n-k} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Devansh
1914078
Dalal (19)

$H = I_{n-k} : P^T$

$$= \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

$CH^T = S$ where S is error syndrome
C is received code word

$$110101 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = (1+0+0+1+0+1),\ (0+1+0+1+0+0),\ (0+0+0+0+0+1)$$

$$= 1, 0, 1$$

$S = (1, 0, 1)$
from syndrome table
$e = 000001$

correct message $= C + e$
$= 110101 + 000001$
$= \underline{110100}$

Devansh
1914078
Delhi

(11)

Q3) $g(x) = x^3 + x + 1 \quad n = 7 \quad k = 4$

(i) message = 0 0 0 1

$M(x) = 1$

$c(x) = x^{n-k} M(x) + p(x)$

$p(x) = \text{remainder}\left(\frac{x^{n-k} M(x)}{g(x)}\right)$

$= \text{rem}\left(\frac{x^3(1)}{x^3 + x + 1}\right)$

$$x^3 + x + 1 \overline{)\,1}$$

$$x^3 + x + 1$$

$$x + 1$$

$p(x) = x + 1$

→ $c(x) = x^{n-k} M(x) + p(x)$

$= x^{7-4}(1) + x + 1$

$= x^3 + x + 1$

$= 0x^6 + 0x^5 + 0x^4 + x^3 + 0x^2 + x + 1$

$= [\,0\ 0\ 0\ 1\ 0\ 1\ 1\,]$

code vector = $[\,0\ 0\ 0\ 1\ 0\ 1\ 1\,]$

→ message = 0011

$M(x) = x + 1$

Devansh
1914078
(12) Dekah

$$c(x) = x^{n-k}(M(x)) + p(x)$$

$$p(x) = \text{rem}\left(\frac{x^{n-k} M(x)}{g(x)}\right)$$

$$= \text{rem}\left(\frac{x^3 (x+1)}{x^3+x+1}\right)$$

$$= \text{rem}\left(\frac{x^4+x^3}{x^3+x+1}\right)$$

$$\begin{array}{r} x+1 \\ x^3+x+1 \overline{)\ x^4+x^3} \\ \underline{x^4+x^2+x} \\ x^3+x^2+x \\ \underline{x^3+x+1} \\ x^2+1 \end{array}$$

$$p(x) = x^2+1$$

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

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

$$= 0x^4+0x^3+x^4+x^3+x^2+0x+1$$

$$c = [0\ 0\ 1\ 1\ 1\ 0\ 1]$$

ii) $g(x) = x^3+x+1$

$$G = [I_k \mid P] = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

$$1st\ row = \text{rem}\left(\frac{x^7-1}{g(x)}\right) = \text{rem}\left(\frac{x^6}{x^3+x+1}\right)$$

(914078
Devansh
Roll no :- (13)

$$x^3+x+1 \overline{)\, x^7 \,} \quad (x^3+x+1$$

$$x^7 + x^5 + x^4$$

$$x^5 + x^4$$

$$x^5 + x^3 + x^2$$

$$x^4 + x^3 + x^2 + x$$

$$x^4 + x^3 + x$$

$$x^3 + x + 1$$

$$x^2 + 1 \quad = [1\ 0\ 1]$$

2nd row $= \text{rem}\left(\frac{x^{7-2}}{g(x)}\right) = \text{rem}\left(\frac{x^5}{x^3+x+1}\right)$

$$x^3+x+1 \overline{)\, x^5 \,} \quad (x^2+1$$

$$x^5 + x^3 + x^2$$

$$x^3 + x^2$$

$$x^3 + x + 1$$

$$x^2 + x + 1 \quad = [1\ 1\ 1]$$

3rd row $= \text{rem}\left(\frac{x^{7-3}}{g(x)}\right) = \text{rem}\left(\frac{x^4}{x^3+x+1}\right)$

$$x^3+x+1 \overline{)\, x^4 \,} \quad (x$$

$$x^4 + x^2 + x$$

$$x^2 + x \quad = [1\ 1\ 0]$$

4th row $= \text{rem}\left(\frac{x^{7-4}}{g(x)}\right) = \text{rem}\left(\frac{x^3}{x^3+x+1}\right)$

$$x^3+x+1 \overline{)\, x^3 \,} \quad (1$$

$$x^3 + x + 1$$

$$x + 1 \quad = [0\ 1\ 1]$$

Devansh
1914078

(14)

$$G = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

(ii) The parity check matrix :-

$$H = [P^T \mid I_{3\times 3}]$$

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \qquad P^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}_{3\times 4}$$

Hence parity check matrix is

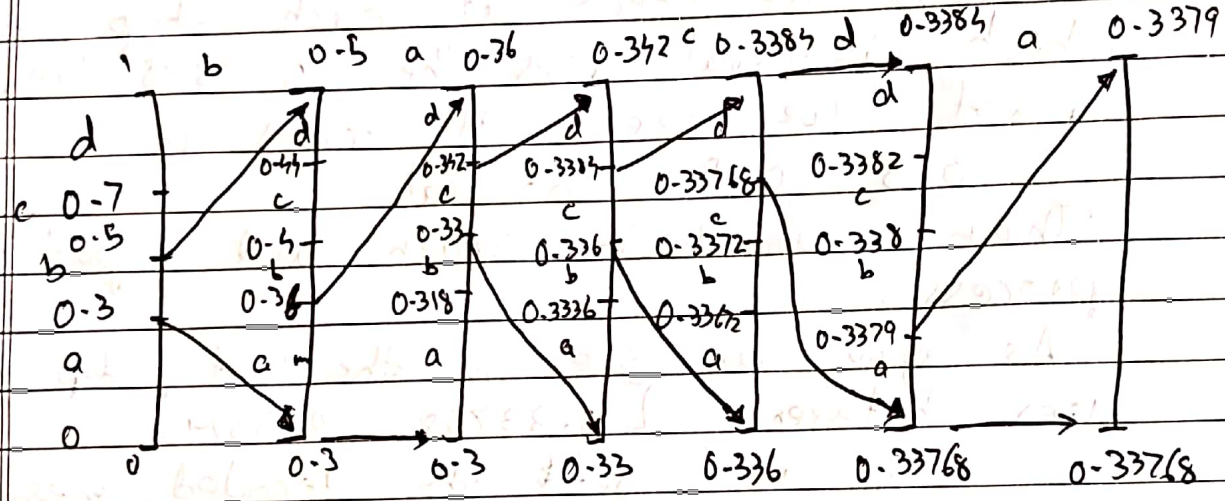
$$H = \left[\begin{array}{cccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]_{3\times 7}$$

Devansh
1914078
Dsluh
13

04) Message : b a cc da

$P(a) = 0.3$
$P(b) = 0.2$
$P(c) = 0.2$
$P(d) = 0.3$

We first divide the interval [0, 1) into four intervals propostional to the probabilities of occurrence of symbols

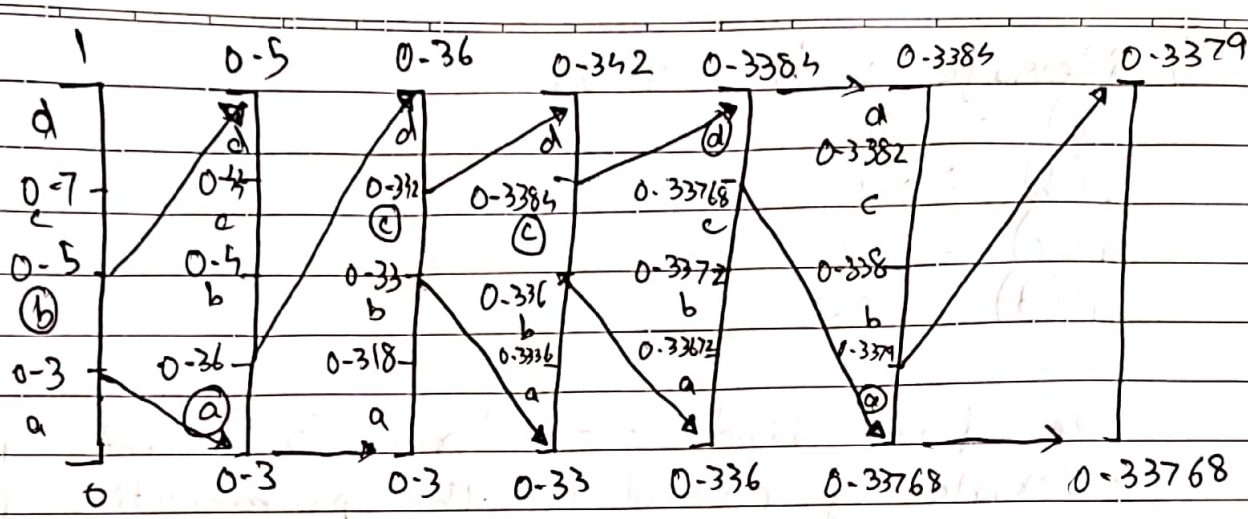


∴ By arithmetic coding, we get the final message symbol to be in the subinterval [0.33768, 0.3379)
Any number within this range will be used to represent the message.

For decoding the message, consider the range given and take any no. say 0.3378
The known probabilities :-

$P(a) = 0.3$ $P(c) = 0.2$
$P(b) = 0.2$ $P(d) = 0.3$

Devansh
1914078
Dehuri



So now we check at each step in which interval does the 0.3378 lie.

First we see it comes in 0.3 - 0.5 interval

Then we check again and repeat the process.

As you can see in the last step, 0.3378 lies between : [0.33768, 0.3379)

∴ we get the decoded message "baccda"