Page

Subject: Computer Network   Sem: V

Assignment 1

Q.1) What are the design issues of layers in OSI reference model of networking?

Ans) The following are the design issues for the layers in OSI reference model of networking:-

1. Reliability: It is a design issue of making a network that operates correctly even when it is made up of unreliable components. e.g:- Routing, error correction and detection.

2. Addressing:- There are multiple processes running on one machine. Every layer needs a mechanism to identify senders and receivers.

3. Error Control:- It is an important issue because physical communication circuits are not perfect. Many error detecting and correcting codes are available. Both send and receiving ends must agree to use any one code.

4. Flow control: If a rate at which data is produced by the sender is higher than rate at which data is received by the receiver, there are chances of swamping the receiver. So, a proper flow control mechanism needs to be implemented.

Date
Page

5.) **Scalability:-** Network sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accomodate such additions and alterations.

6.) **Resource Allocation:-** Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and de-allocate resources to processes, optimal usage of the resources

7.) **Statistical Multiplexing:-** It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of bandwidth or time to each host.

8.) **Routing:-** There may be multiple paths from the source to destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

Date
Page

9.) Security (Confidentiality & Integrity):- A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography. Mechanisms that provide confidentiality defend against threats like eaves dropping. Mechanisms for integrity prevent faulty changes to messages.

Q.2) Write a short note on Twisted Pair, Coaxial Cable.

Ans) (I) Twisted-Pair Cable:-

(1) One of the earliest guided transmission media is twisted pair cables. A twisted pair cable comprises of two seperate insulated copper wires, which are twisted together and run in parallel.

(2) The copper wires are typically 1mm in diameter

(3) One of the wires is used to transmit data & the other is the ground reference.

(4) Reason for Twisting:- (i) All transmissions are prone to noise, interferences, and cross talks.

(ii) When the wires are twisted, some part of the noise signals is in the direction of data signals while the other parts are in the opposite directions. Thus the external waves cancel out due to different twists.

(iii) The receiver calculates the difference in the

Voltages of two wire for retrieving data. Thus, a much better immunity against noise is obtained.

(5) Application:- (i) In LANs (ii) In DSL lines (iii) In telephone lines.

(6) Types:- (i) Unshielded Twisted Pair (UTP):- These generally comprise of wires & insulators.
(ii) Shielded Twisted Pair (STP):- They have a braided wired mesh that encases each pair of insulated wires.

(7) Categories:- (i) CAT-1:- UTP, B.W < 0.1 Mbps
(ii) CAT-2:- UTP, B.W ≤ 2 Mbps
(iii) CAT-3:- UTP, B.W ≤ 10 Mbps
(iv) CAT-4:- UTP, B.W ≤ 20 Mbps
(v) CAT-5:- UTP, B.W ≤ 10^2 Mbps
(vi) CAT-6:- UTP, B.W ≤ 2×10^2 Mbps.

(II) Coaxial Cable:-
(1) Coaxial cables, commonly called coax, are copper cables with metal sheilding designed to provide immunity against noise and greater bandwidth.
(2) Coax transmit signals over larger distances at a higher speed as compared to twisted pair cables.
(3) Structure:- (i) Coax has a central core of stiff copper conductor for transmitting signals. This is covered by an insulating material.
(ii) The insulator is encased by a closely woven

braided metal outer conductor that acts as a shield against noise.

(iii) The outer conductor is again enclosed by a plastic insulating cover.

(4) **Categories**:- Coaxial cables are categorized into three types as per radio government (RG) ratings:- (i) RG-59: Z = 75 W, used = Cable TV

(ii) R.G-58: Z = 50 W, used = Ethernet.

(iii) R.G-11: Z = 50 W, used = thick Ethernet.

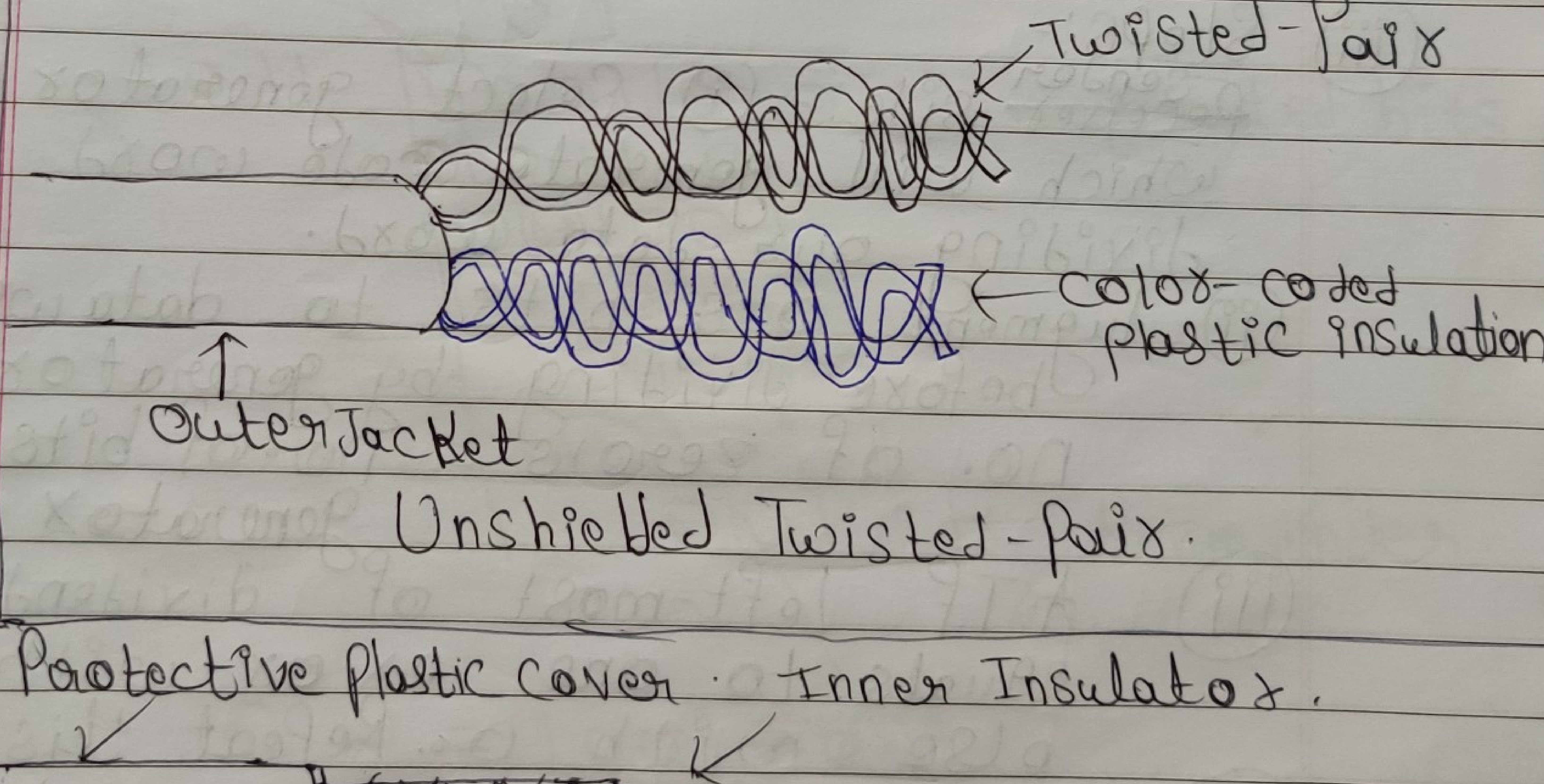
(5) **Applications**:- (i) In analog telephone networks.

(ii) In digital telephone networks (< 600 Mbps).

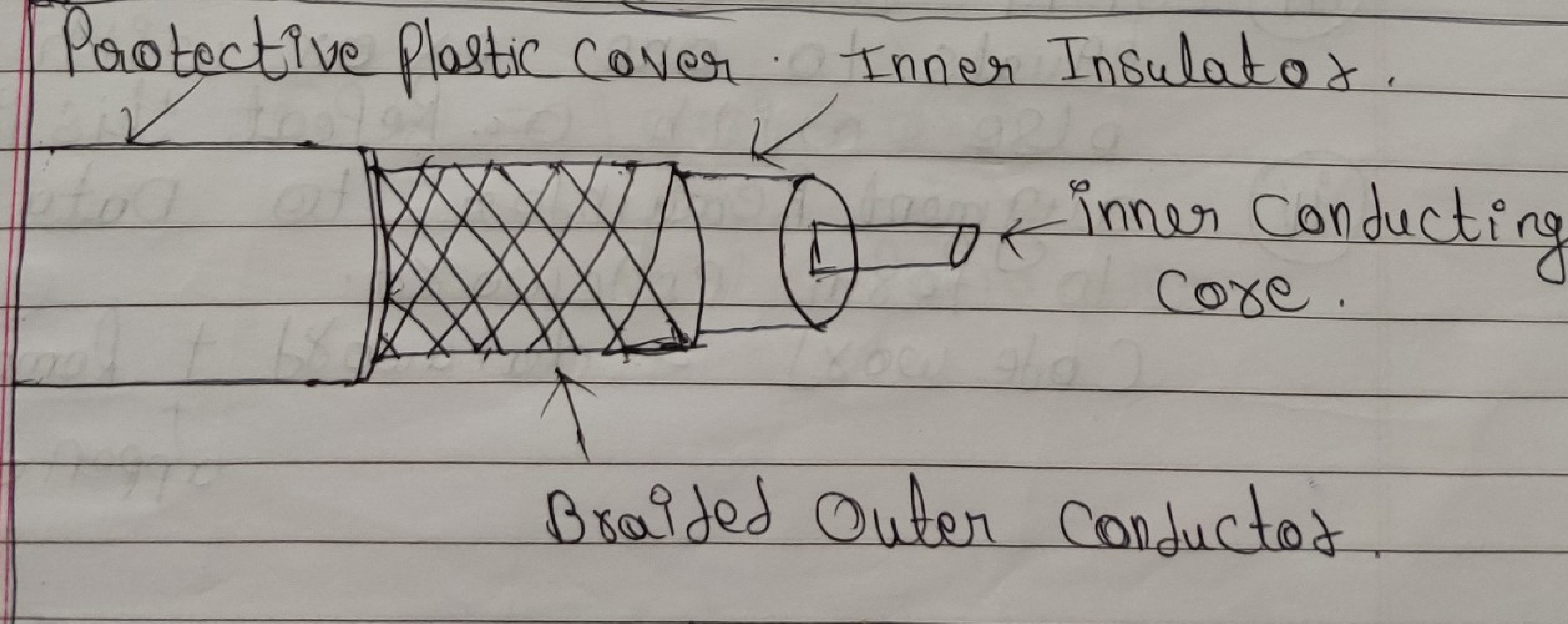
(iii) Cable TV networks.

(iv) Ethernet LANs.

(v) In MANs.



Unshielded Twisted-Pair.



Coaxial cable.

Date
Page

Q.3) Explain different error detection techniques with example.

Ans) (I) Cyclic Redundancy Check (CRC):-

(i) Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a code word is cyclically shifted (rotated), the result is another code word.

(ii) A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data.

(iii) Steps:-

~~Receiver~~ Sender side:- (i) Select generator polynomial which will generate code word by dividing our data word.

(ii) Augment 0's bits to data word before dividing by generator
no. of zero's = no. of bits in generator - 1

(iii) ~~A~~ If left-most of dividend equals to one ex-or with divisor else with 0. Repeat this procedure.

(iv) augment Remainder to Data word to form codeword.

Code word = dataword + Remainder.
↑
append.

Receiver Side:- (i) Divide the code-word received from generator using Step-3 from Sender Side.

(ii) If Remainder or Syndrome is 0 then Code-word received in correct remove no. of bits in generator - 1 ~~to~~ from C.W to form data word.

(iii) If Remainder is not zero received C.W is incorrect ask for retransmission.

e.g.:-

D.W = 1001 ; Generator = 1011

C.W :- ?

```
                 D.W
                 101
G(x) → 1011 ) 1001 | 000 |  ← augmented bits
              1011
              ------
              00100
              0000
              ------
               01000
               1011
              ------
              0 | 011 |  ← Remainder.
```

∴ C.W = 1001 011

1001 ↑ D.W ; 011 ↑ Remainder

e.g.:- D.W = 1001 ; Generator = 1011

```
              1010
G(x)  1011 ) 1001|000   ← augmented-bits
             1011↓
             0100
             0000↓
              1000
              1011↓
              0110
              0000
               110      ← Remainder.
```

∴ C.W = 1001110 ← Remainder.

↑ D.W

Receiver Side:-

without error

C.W = 1001110

```
          1010
   1011 ) 1001110
          1011↓
          0101
          0000↓
           1011
           1011↓
           0000
           0000
            000   ← Syndrom=0
```

∴ D.W = 1001

with error.

C.W = 1000110

```
          1011
   1011 ) 1000110
          1011↓
          0111
          0000↓
           1111
           1011
           1000
           1011
            011
```

Syndrome ≠ 0

ASK for retransmission.

Date
Page

(II) Check Sum:-
Steps:-

1. At the Source, the message is first divided into m-bits units.
2. The generator then creates the checksum i.e an extra m-bits unit.
3. At destination, the checker creates a new checksum from the combination of the message & sent checksum.
4. If check sum is 0 then message is accepted else message is discarded.

e.g:-
Sender:-

7
11
12 max-bits = 4
0
6
+ $\boxed{0}$ ← extra bit will be replaced with Check-sum bits.
←36

$\boxed{1\,0\,0\,1\,0\,0}$
$+\ 4 \longrightarrow 10$
$6 = 0110 \xrightarrow{1's} 1001 = 9$

∴ Packet = 7, 11, 12, 0, 6, $\boxed{9}$

Date
Page

Receiver:-

$$
\begin{array}{r}
7 \\
11 \\
12 \\
0 \\
6 \\
+ \quad \boxed{9} \\
\hline
45
\end{array}
$$

max-bits = 4

$45 \leftarrow 10\ \boxed{1101}$

$10 \rightarrow 10$

$15 = 1111 \xrightarrow{\text{1's Comp}} 0000 = 0$

∵ Check-sum = 0
Received packet is correct.

∴ Required-info = 7, 11, 12, 0, 6

Q.3) ① Hamming Code is used for error detection as well as error correction in for data frame.

② It does so my adding 'r' redudant bit in actual frame.

③ Let, us see how it encode by example:-

④ Consider, we have data frame (dw) as 1001011

⑤ Total ~~length~~ length $l(dw) = m = 7$

⑥ we add 'r' redundant bit by following formula :- $m <= 2^r - r - 1$
we can observe that $r=4$ is suited for above formula
$m <= 2^4 - 4 - 1 <= 11$

⑦ We insert r bits at the position of power of i.e $2^0, 2^1, 2^2, 2^3$
P_1 P_2 P_4 P_8

⑧ Total bit of encoded word is $n = m + r$
i.e $n = 7 + 4 = 11$

⑨ encoding :-

D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	0	1	1	0	1	0	1	1	0

Table - a

we insert Dw bits at D position sequenti-ally & encode value of P using even parity by selecting 2^r alterate bits.

$P_1 = P_1\ D_3\ D_5\ D_7\ D_9\ D_{11} = 0$
$P_1\ 1\ 1\ 1\ 0\ 1\ 1$
$\therefore$ even parity $P_1 = 0$

$P_2 = P_2\ D_3\ D_6\ D_7\ D_{10}\ D_{11} = 1$
$P_2\ 1\ 0\ 1\ 0\ 1\ 0$
$\therefore$ odd parity $\therefore P_2 = 1$

$P_4 = P_4\ D_5\ D_6\ D_7 = 0$
$P_4\ 1\ 0\ 1$
$\therefore$ Even parity $\therefore P_4 = 0$

$P_8 = P_8\ D_9\ D_{10}\ D_{11} = 1$
$P_8\ 0\ 0\ 1$
$\therefore$ odd parity $\therefore P_8 = 1$

~~$\therefore$ C.W = 0110~~
$\therefore$ C.W = 10011010110
This will be send to receiver

(10) Receiver side Decoding: Receiver used reversed engineering to form dw from the code and check if any error is detected & if detected it will correct it.

(11) Receiver will decode C.W in following way (referencing table a):-

$P_1 = P_1\ D_3\ D_5\ D_7\ D_9\ D_{11} = 0$ ✓
$1\ 1\ 1\ 0\ 1$

$P_2 = P_2\ D_3\ D_6\ D_7\ D_{10}\ D_{11} = 1$ ✓
$P_2\ 1\ 0\ 1\ 0\ 1$

$P_4 = P_4\ D_5\ D_6\ D_7 = 0$ ✓
$P_4\ 1\ 0\ 1$

$P_8 = P_8\ D_9\ D_{10}\ D_{11} = 1$ ✓
$P_8\ 0\ 0\ 1$

we See all the bits are correct now we remove Parity bits & form original d.w = 1001011

(12) If any bit was inverted we have gotten wrong parity for it.

(13) For detecting wrong parity we select common bits from parity encoding i.e, for $P_1 \circ P_2 \circ P_4 = D_7$ & so on.

(14) So, we will invert the common bit, & we will have our right code.

(15) we can also add Parity bits to check where the error is
i.e $1+2+4 = 7^{th}$ bit.