HANU
HANOI UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

Fall, 2023

# DISCRETE MATHEMATIC LEC-08:

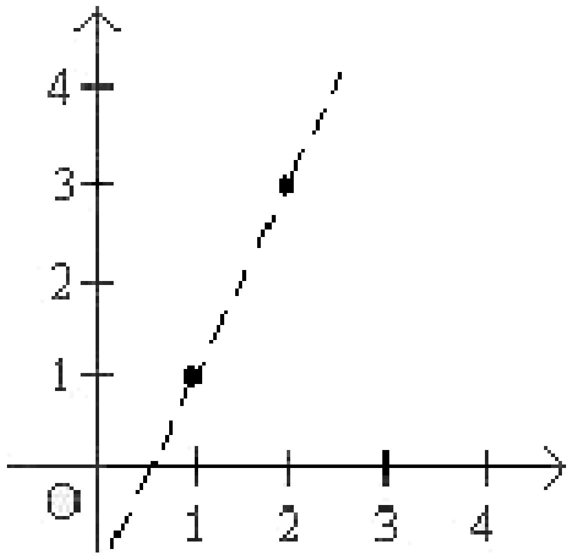
## Error Correcting Codes

# Recall Property of Polynomial

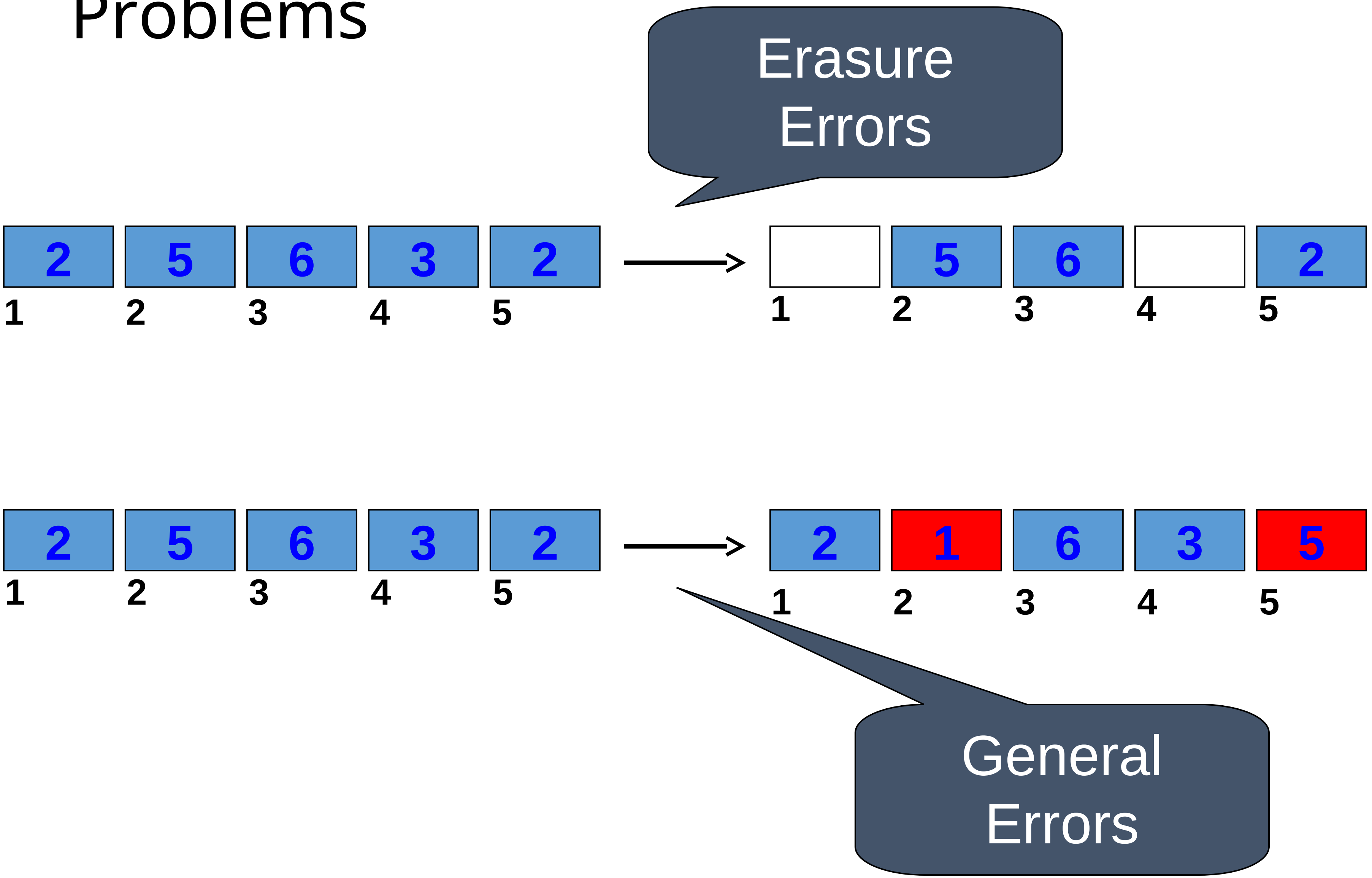
Given $d$+1 pairs $(x_1,y_1)$, $(x_2,y_2)$…, $(x_{d+1},y_{d+1})$, there is a unique polynomial of degree (at most) $d$: $P(x_i)=y_i$ $(1 \le i \le d+1)$

***d* = 1: two points determine a line**

***d* = 2: three points determine a polynomial of degree at most 2**



# Problems

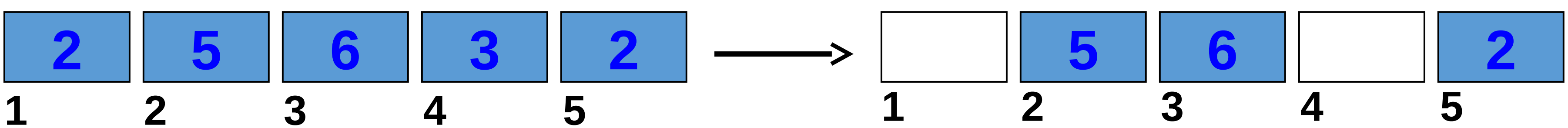

Erasure Errors
2
5
6
3
2
1
2
3
4
5
5
6
2
1
2
3
4
5
2
5
6
3
2
1
2
3
4
5
2
1
6
3
5
1
2
3
4
5
General Errors

# Solution

- Error Correcting Codes (ECC)
  - Redundancy

# 1. Erasure Errors

Example: transmitting information (i.e. a file) on an unreliable channel (i.e. the internet), where the file is broken up into n packets, and some of the packets are lost during transmission.



# Solution

- Step 1: The sender finds a polynomial degree (n-1), which when evaluated at different points will give the contents of all packets.

➢ For example: when sending 3 numbers 1, 4 and 9, a polynomial $P(x)= x^2$ can be used to store the information of packets, because $P(1)=1$, $P(2)=4$ and $P(3)=9$.

- Step 2: The sender sends extra packets number of which is equal to that of lost ones (k).

➢ Example: Packet "1" is lost during transmission, so the sender evaluates P(x) at 1 additional point, say x=4, to have an extra packet which is "16".

- Step 3: The recipient reconstructs the polynomial from the n received packets using Lagrange interpolation.

- Is it possible?.

# Example

- Packets 2, 4, 8. (2 lost)
- Consider $P(1)=2$, $P(2)=4$, $P(3)=8$
- Find $P(x) = x^2 - x + 2$
- Send $P(1)=2$, $P(2)=4$, $P(3)=8$, $P(4)=14$, $P(5)=22$
- Receive $P(2)=4$, $P(4)=14$, $P(5)=22$
- Reconstruct $P(x) = x^2 - x + 2$
- Recover $P(1)=2$, $P(3)=8$

# 2. General Errors

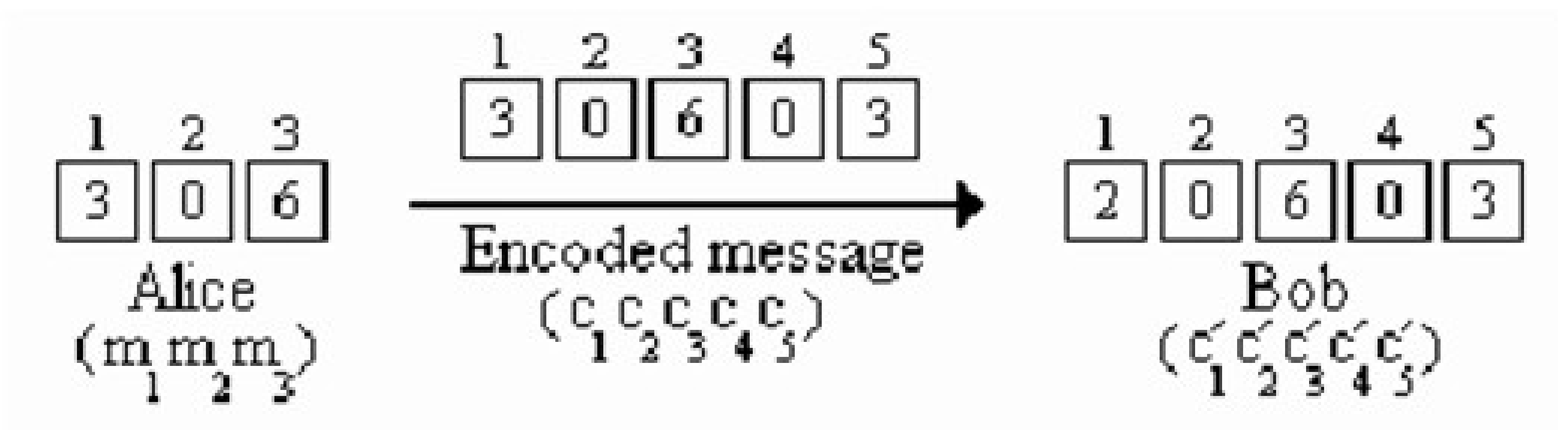
Example: transmitting information on an unreliable channel where the file is broken up into n packets, and the contents of some packets are changed during transmission.

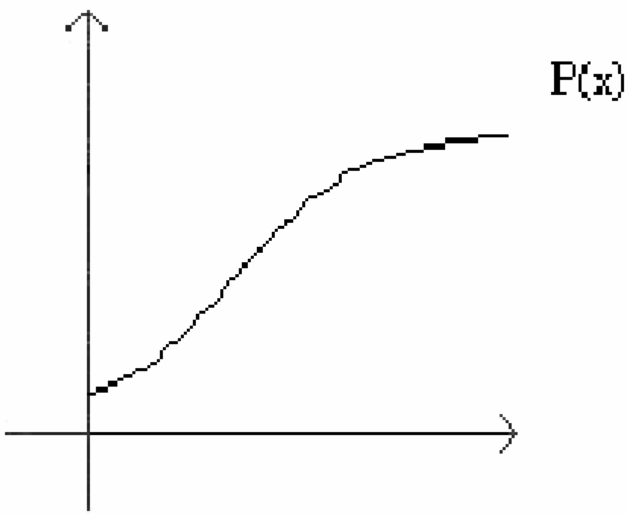
# Solution

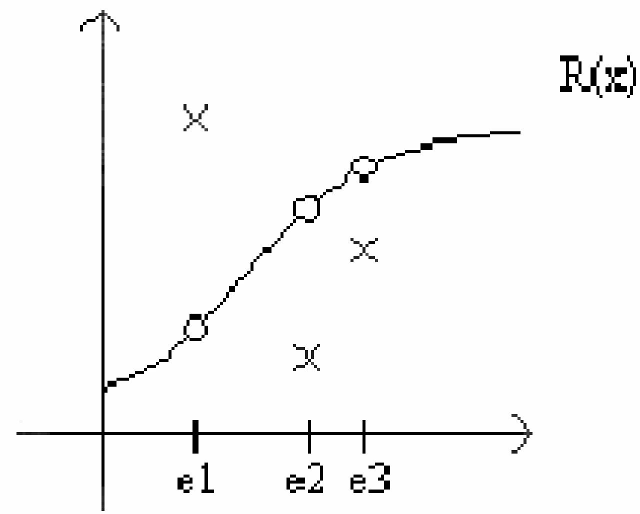
- Step 1: Similar to erasure error solution (finding a polynomial P(x)).
- Step 2: The sender sends the number of extra packets (2k) which doubles the number of altered ones (k).

E.g (continued from the above one): the packet “1” is changed into “-1” so 2 more packets need to be sent, say 25 and 36

- Step 3: The recipient reconstructs the polynomial from the n+2k received packets.




P(x)


R(x)
e1
e2
e3

- The problem is the locations of the k errors. We could try to guess where they lie, but this would take too long and can be impossible with large polynomials. Consider the error-locator polynomial:

  $E(x) = (x-e_1)*(x-e_2)\ldots*(x-e_k)$

  which has degree k (since x appears k times)

- Important observation:

  P(x) *E(x) =R(x) *E(x)

  Note: P(x) is the original polynomial, and R(x) is the function which contains n+2k received packets including the corrupted ones.

- Let P(x)*E(x)=Q(x)

$$Q(x) = a_{n+k-1}x^{n+k-1} + \cdots + a_1 x + a_0$$

$$E(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$$

- Replacing x with all n+2k values (the points that were evaluated to give contents of the packets), we have n+2k linear equations with n+2k variables:

  $Q(x_1) = R(x_1) * E(x_1)$

  $Q(x_2) = R(x_2) * E(x_2)$

  ………………

  $Q(x_{n+2k}) = R(x_{n+2k}) * E(x_{n+2k})$

- Note that at this point, the n+2k variables are

$$a_{n+k-1}, \quad . \quad . \quad . \quad , a_0$$

  and

$$b_{k-1}, \quad . \quad . \quad . \quad , b_0.$$

  solving the equations, we find the coefficients of E(x) and Q(x), whose ratio is P(x).

# For your interest

- n=3, k=1
- If you receive 5 values:

  0 2 6 12 10

  What is P(x)? Which packet was changed?