Discrete Structures

Day 4

Error detection using Cyclic Redundancy code (CRC)

- Message to be transmitted
  - Eg: 1011011
- Generator known to both sender and receiver. Let ‘n’ be the length of the generator.
  - Eg: 1101 here n = 4
- Pad n-1 bits as 0’s to the message to be transmitted
  - Padded message: 1011011000
- Finding the CRC: Divide the padded message by generator. Reminder is obtained by performing XOR operation

1101	1011011000 (Padded message)
	1101
	1100
	1101
	1110
	1101
	1100
	1101
	001 (CRC)

1101	1011011001 (Without error)
	1101
	1100
	1101
	1110
	1101
	1101
	1101
	000 (CRC)

1101	1010011001 (With error)
	1101
	1110
	1101
	1111
	1101
	1000
	1101
	1011
	1101
	110(CRC)

Sender:
Message is sent as: 1011011001

Receiver:
CRC=000 No error is received data

Receiver:
CRC≠000 Error is received data

Single bit error detection and correction using Hamming code

- Hamming code developed by R.W. Hamming.
- It pads 'p' parity bits to 'n' number of data bits which follows the eqn.: $2^p \geq n + p + 1$
  - Eg: If n=4, p =3
- The parity bits are placed at 2^i positions
  - Eg: Data bits to be transmitted: 1101
  -

1	1	0		1		
7	6	5		3		

$$\boldsymbol{p_1} \rightarrow \mathbf{1, 3, 5, 7}$$
$$\boldsymbol{p_2} \rightarrow \mathbf{2, 3, 6, 7}$$
$$\boldsymbol{p_4} \rightarrow \mathbf{4, 5, 6, 7}$$

Calculate parity bits as odd/even parity

1	1	0		1		
7	6	5	4	3	2	1

Assume even parity (even number of 1's):

$$\boldsymbol{p_1} = \mathrm{x}, 1{,}0{,}1 = 0$$
$$\boldsymbol{p_2} = \mathrm{x}, 1{,}1{,}1 = 1$$
$$\boldsymbol{p_4} = \mathrm{x}, 0{,}1{,}1 = 0$$

1	1	0	0	1	1	0

Sent to the receiver

Error position			
0(no error)	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1

Case1: Received with no error

1	1	0	0	1	1	0

Check:

$$\boldsymbol{c_1} = 0, 1,0,1 = 0$$

$$\boldsymbol{c_2} = 1, 1,1,1 = 0$$

$$\boldsymbol{c_4} = 0, 0,1,1 = 0$$

- $\boldsymbol{c_4 c_2 c_1}$:000 (no error)

Case2: Received with single bit error

1	1	0	1	1	1	0

Check:

$$\boldsymbol{c_1} = 0, 1,0,1 = 0$$

$$\boldsymbol{c_2} = 1, 1,1,1 = 0$$

$$\boldsymbol{c_4} = 1, 0,1,1 = 1$$

- $\boldsymbol{c_4 c_2 c_1}$:100 (Error at position $(100)_2 = 4_{10}$)
- The corrected code will be:

1	1	0	0	1	1	0

- Detect if any error and correct if required in the Hamming code:

1	1	0	0	1	0	1	0	0

Cryptography

- Transforming information so that it cannot be easily recovered without special knowledge.

- **Classical Cryptography**
- One of the earliest known uses of cryptography was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet
- $f(p) = (p + 3) \textbf{ mod } 26.$
- Encryption: The process of making a message secret i.e. converted a plain text to cipher text. Eg: YOU(plaintext) BRX(ciphertext)
- Decryption: The process of converting a cipher text to plain text.

Q. What is the secret message produced from the message "PARK" using the Caesar cipher? (Assume A, B, C, . . . , Z = 0, 1, 2, . . ., Z)

- PARK integer representation: 15, 0, 17, 10
- $f(p) = (p + 3)$ **mod** 26

  18, 3, 20, 13

  S D U N

Q. What is the plain message if the cipher text is "WKH" encrypted using Caesar cipher?

- **CRYPTANALYSIS** The process of recovering plaintext from ciphertext without knowledge of both the encryption method and the key is known as **crytanalysis** or **breaking codes**.

- Cryptanalysis of messages that were encrypted using a shift cipher

- The nine most common letters in English text and their approximate relative frequencies are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%
- Suppose that we intercepted the ciphertext message ZNK KGXRE HOXJ MKZY ZNK CUXS that we know was produced by a shift cipher. What was the original plaintext message?

- The most common letter in the ciphertext is K.
- Hypothesize that the shift cipher sent the plaintext letter E to the ciphertext letter K (6 shift, key=6)

A	B	C	D	E	F	G	H	I	J	K	.	.	.	.	Z
0	1	2	3	4	5	6	7	8	9	10	.	.	.	.	25

- Shift the letters of the message by −6, obtaining THE EARLY BIRD GETS THE WORM