Ministry of Higher Education and Scientific Research

Al-Furat Al- Awsat Technical University

Engineering Technical college / Najaf

Communication Engineering Department

Information Technology (CE231)

2nd Class 2018/2019

Lecturer Ali M. Alsahlany

Lecture Outlines :

- **Introduction**
- **Error detection codes**
  - **Error detection codes / parity codes**
- **Error correction codes**
  - **Error correction codes / Basic definitions**
  - **Error Correction Codes / Hamming Codes**
  - **Error Correction Codes / Cyclic Codes**

Channel Coding: *To ensure reliable communications, techniques have been developed that allow bit errors to be detected and corrected. The process of error detection and correction involves adding extra redundant bits to the data to be transmitted. This process is generally referred to as channel coding.*

Channel coding methods fall into to two separate categories:

- ***Error detection codes:*** *only have the ability to confirm that bit error(s) has occurred, however they cannot tell you which bit was in error. To fix the error, the receiver must request a retransmission.*
- ***Error correcting codes or forward error correction (FEC) codes:*** *have the ability to detect some bit errors and fix them without requiring a retransmission.*

Block Codes **In block codes, the encoder takes in k information or message bits and produces a codeword of length $n = k + r$. Since $k + r > k$, the quantity r represents the number of extra bits (redundancy) added. This would be referred to as an (n, k) linear code.**

$n = k + r$

k: $bit\ in\ data$

r: $rudandanc\ bit$

$n = codeword\ bit$

k information bit $\longrightarrow$ **Encoder** $\longrightarrow$ *Codeword of length $k + r$*

__Example 1__: Linear block code (7,4) with k= 4 and k + r = 7

Message	Code words
(0 0 0 0)	(0 0 0 0 0 0 0)
(0 0 0 1)	(1 0 1 0 0 0 1)
(0 0 1 0)	(1 1 1 0 0 1 0)

A key point about channel coding is that there is a cost to be paid of increasing reliability. The extra n bits added by encoding result in:

- *Larger file sizes for storage.*
- *Higher required transmission data rates.*

This cost is represented by __the code rate.__ The code rate R_c is the ratio of the number of information bits k to the number of bits in the codeword k + r.

$$R_c = k/n$$

$$\overbrace{\boxed{r \text{ bits (add redundancy)}}\boxed{k \text{ bits (information or message bit)}}}^{n = k + r}$$

***Example 2**: code (8,7)*
That is mean n = 8bit, k = 7bit, and r = 8 – 7 = 1bit
$R_c = k/n = 7/8$

Simple Error Detection Codes:

Parity codes The simplest kind of error-detection code is the *parity code*. To construct an even-parity code, add a parity bit such that the total number of 1's is even.

Parity check code (n , k)
$R_c = k/(k+1)$

Information bits	Even parity code	Odd parity code
000	000 **0**	000 **1**
001	001 **1**	001 **0**
010	010 **1**	010 **0**
011	011 **0**	011 **1**

1-bit parity codes can detect single bit errors, but they do not detect 2 bit errors.
Probability (detecting errors)= Probability (odd number of errors) and
Probability (undetecting errors)= Probability (even number of errors).

Example 3: Parity check code of k=7 bit. Calculate P (undetected error) and P (detected error)

Solution:

P (undetect error) $= \sum C_k^n p^k (1-p^k) = C_2^8 p^2 (1-p)^6 + C_4^8 p^4 (1-p)^4 + C_6^8 p^6 (1-p)^2 + C_8^8 p^8 \approx 28x10^{-4}$

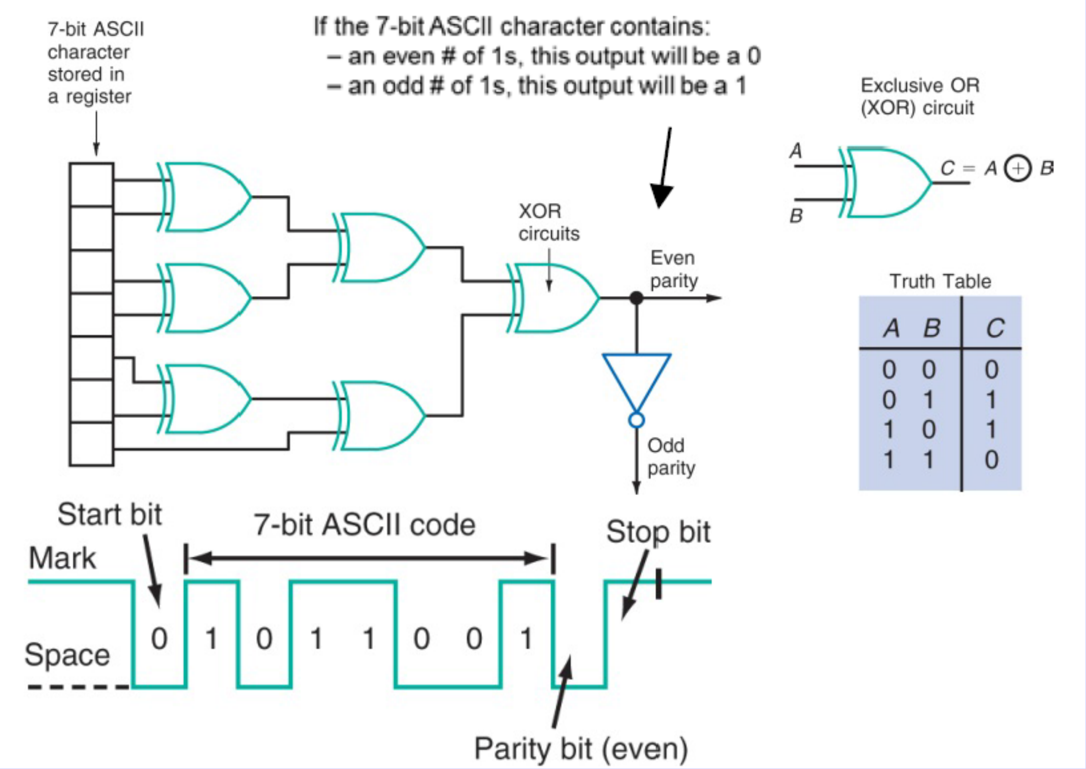
The probability of detected errors will be:

P (detect error) $= \sum C_k^n p^k (1-p^k) = C_1^8 p^1 (1-p)^7 + C_3^8 p^3 (1-p)^5 + C_5^8 p^5 (1-p)^3 + C_7^8 p^7 \, (1-p) \approx 8x10^{-3}$

Homework1: *assume there are n=12bits in a codeword (packet). Probability of error in a single bit transmission* p_b=10^{-3}. *Find the probability of error-detection failure.*

To implement these parity generators, simple Ex-OR gates are used at TX and RX as shown below

Information bits	Even parity code
1010111	1
0110101	0



***Example 4**: Parity cheak code (8,7) find code word if data* $I_1 = [0111010], I_2 = [1100111],$ *and* $I_3 = [0000000]$.

Solution:

$C_i = [I_i : parity\ bit]$

$C_1 = [01110100]$ $C_2 = [11001111]$ $C_2 = [00000000]$

***Excersise 1**: detect error in the received code word (use parity check code (8,7) then find data words.*

$C_1 = [01010101]$ $C_2 = [00000001]$ $C_3 = [11110110]$

Solution:

- *In code* C_1 *number of ones is even there is no error, data is 0101010*
- *In code* C_2 *number of ones is odd there is error*
- *In code* C_3 *number of ones is even there is no error, data is 1111011*

Systematic and nonsystematic codes: ***If information bits (a 's) are unchanged in their values and position at the transmitted codeword, then this code is said to be systematic.***

Input data [D]= $[a_1\ a_2\ a_3\ \dots\dots\dots\ a_k]$,

Output systematic (n,k) codeword is [C] = $[a_1\ a_2\ a_3\ \dots\dots\dots\ a_k\ c_1\ c_2\ c_3\ \dots\dots\dots\ c_r]$

However if data bits are spread or changed at the output codeword then, the code is said to be nonsystematic:

Output nonsystematic (7,4) codeword is [C] = $[c_2\ a_1\ c_3\ a_2\ c_1\ a_4\ a_3]$

Hamming distance: ***The ability of error detection and correction codes depends on this parameter. The Hamming distance between two codewords*** c_i ***and*** c_j ***is denoted by*** d_{ij} ***which is the number of bits that differ. For a binary (n,k) code with*** 2^k ***possible codeword then the minimum Hamming distance (HD) is the min)*** (d_{ij}) ***of course*** $n \geq d_{ij} \geq 0$

Example 5: ***Find the Hamming distance between the two codewords:***
$C_1 = [1011100]$ ***and*** $C_2 = [1011001]$.
Solution: ***Here, the number of bits that differ is 2, hence*** $d_{12} = 2$

Homework 2: ***Find the minimum Hamming distance for the 3 codewords.***
$C_1 = [1011100]$, $C_2 = [1011001]$, $C_2 = [1011000]$

Hamming weight: ***This is the number of 1's in the non zero codeword*** c_i. ***It is denoted by*** w_i. ***As will be shown later, and for linear codes,*** $w_{min} = HD = \min(d_{ij})$. ***This simplifies the calculation of HD. As an example 5,***
Example 6: ***If*** $C_1 = [1011000]$ ***, then*** $w_i = 3$, ***for*** $C_2 = [0001010]$, ***then*** $w_i = 2$ ***and so on.***

Linear and non Linear codes: ***when the parity bits are obtained from a linear function of the k information bits then the code is said to be linear, otherwise it is a nonlinear code.***

Hamming Bound: The purpose of Hamming bound is either

1) to choose the number of parity bits (r) so that a certain error correction capability is obtained. Or

2) to find the error correction capability (t) if the number of parity bits (r) is known for binary codes, this is given by:

$$2^{n-k} = 2^{r} \geq \sum_{j=0}^{t} C_j^n$$

where t is the number of corrected bits.

$$t = int[\frac{HD-1}{2}]$$

$$no. of\ detected\ error\ bit = HD - 1$$

Example 7: for a single correction code with k=4 find the no. of parity bits that should be added.

Solution:

$2^{r} \geq \sum_{j=0}^{1} C_j^{4+r} = C_0^{4+r} + C_1^{4+r}$ This gives $2^r \geq 1+(4+r)$ and the minimum r is r=3

(take minimum r to have max code efficiency). This is the (7,4) code. the code is said to be perfect code.

Homework 3: if k=5 and up to 3 errors are to be corrected, find the no. of check bits that should be added.

Note: If the (n,k) codewords are trans. through a channel having error prob=p_e, then prob. of decoding a correct word at the Rx for t-error correcting code will be:
P(correct words)=p(no error)+p(1 error)+……..p(t errors)
and prob(erroneous word)=1-P(correct word).

Excersise 2: $If\ Code\ of\ t = 2\ , n = 31\ \ find\ \ k$

Solution: $n = 31 \quad k = ? \quad r = ?$

$$2^r \geq \sum_{j=0}^{t} C_j^n$$

$$2^r \geq C_0^{31} + C_1^{31} + C_2^{31}$$

$$2^r \geq 1 + 31 + \frac{31*30}{2}$$

$$2^r \geq 497 \Rightarrow\Rightarrow \quad r \geq 8.95$$

n=31 r =9 k=22bit

Code (31,22)

$$t = 2 \Rightarrow\Rightarrow t = int\left[\frac{HD-1}{2}\right] \Rightarrow\Rightarrow HD = 5$$

No. of detected error= $(HD - 1) = 4bit$

$$P(correct\ error) = \sum_{i=0}^{t} C_i^n P^i (1 - P)^{n-i}$$

$$P(correct\ error) = C_0^{31} P^0 (1 - P)^{31} + C_1^{31} P^1 (1 - P)^{30} + C_2^{31} P^2 (1 - P)^{29}$$

Example 8: Block code (7, 4) calculate no. detect and correct bit Hamming Distance (HD) and P(correct error).

Solution: $n = 7 \quad k = 4 \quad r = 7 - 4 = 3\ bit$

$$2^r \geq \sum_{j=0}^{t} C_j^n$$

$$2^3 \geq \boxed{C_0^7 + }C_1^7 + C_2^7 \ \ldots\ldots$$

$$8 \geq 1 + 7 + \frac{6 * 7}{2} \ldots\ldots$$

Taken two element that mean $t = 1$

$$t = int\left[\frac{HD - 1}{2}\right] \Rightarrow\Rightarrow HD = 3$$

No. of detected error= $(HD - 1) = 2$

$$P(correct\ error) = \sum_{i=0}^{t} C_i^n P^i (1 - P)^{n-i}$$

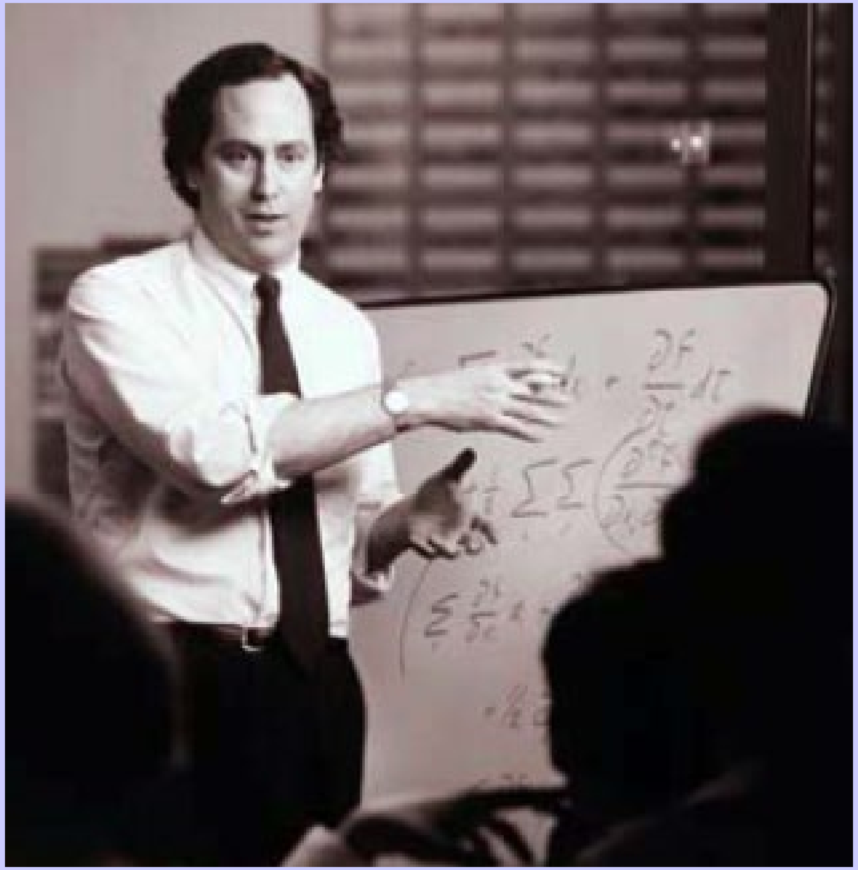
$$P(correct\ error) = C_0^7 P^0 (1 - P)^7 + C_1^7 P^1 (1 - P)^6$$

$$= 1 * 1(1 - P)^7 + 7\mathrm{P}(1 - P)^6$$

$$\text{Code rate} = \frac{k}{n} = \frac{4}{7}$$

One way to detect and correct errors is to add parity checks to the codewords:

- **If we add a parity check bit at the end of each codeword we can detect one (but not more) error per codeword.**
- **By clever use of more than one parity bits, we can actually identify where the error occurred and thus also correct errors.**
- **Designing ways to add as few parity bits as possible to correct and detect errors is a really hard problem.**



Richard W. Hamming (11.2.1915-7.1.1998)

Linear Block Codes:

Only systematic binary codes will be described. The r parity bits are obtained using a linear function of the a's data. Mathematically, this can be described by the set of equations:

$$C_1=h_{11}a_1+h_{12}a_2+h_{13}a_3+\dots\dots+h_{1k}a_k$$
$$C_2=h_{21}a_1+h_{22}a_2+h_{23}a_3+\dots\dots+h_{2k}a_k$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \qquad \dots\dots\dots\dots\dots(1)$$
$$C_r=h_{r1}a_1+h_{r2}a_2+h_{r3}a_3+\dots\dots+h_{rk}a_k$$

Where + is mod-2 addition (EX-OR), product is the AND multiplication and h_{ij} coefficients are binary variables for a binary coding. The complete output codeword can be written in matrix form as:

$\boxed{[C]= [D][G]}$ ....(1) , where:

$$[G]=\begin{bmatrix} 1 & 0 & 0 & 0 & h_{11} & h_{21} & h_{31} & . & h_{r1} \\ 0 & 1 & 0 & 0 & h_{12} & h_{22} & h_{32} & . & h_{r2} \\ 0 & 0 & 1 & 0 & . & . & . & . & . \\ 0 & 0 & 0 & 1 & h_{1k} & h_{2k} & h_{3k} & . & h_{rk} \end{bmatrix}$$

G= [I_k : P_{kxr}] which is kxn matrix.

This matrix is called the generator matrix of the linear block code (LBC). Equation(1) can also be written in matrix form as:

$\boxed{[\,H\,]\,[C]^T=[0]}$ ……………………….(2)

where: $[C]=[\,a_1\; a_2\;\; a_3 \,\ldots\ldots.a_k\; c_1\;\; c_2\; c_3\,\ldots\ldots.c_r]$ and [H] matrix is in fact related with [G] matrix by:

$[\,H\,]=[-P^T : I_r]$, and for binary coding this – sign drops out. This rxn [H] matrix is called the parity check matrix. As will be shown, encoding can be done either using eq(1) ([G] matrix) or eq(2) ([H] matrix), but decoding is done using [H] matrix only.

Example 9: a given binary (7,4) Hamming code with a parity check matrix:

$$G=\begin{bmatrix}1000011\\0100101\\0010110\\0001111\end{bmatrix} \qquad G=[I_{kxk} : P_{kxr}]$$

Find: 1) no. of error correction and detect capability 2) Code rate 3) encoder circuit 4) if data [1011] find codewords.

Solution: n=7 k=4 r=3

$$\left.\begin{array}{c} 2^r \geq \sum_{j=0}^{t} C_j^7 \\ \\ t = 1 \,, HD = 3 \\ No.of\ detect\ error = HD - 1 = 2 \end{array}\right\}$$ **From example 8**

$$C = D.G$$

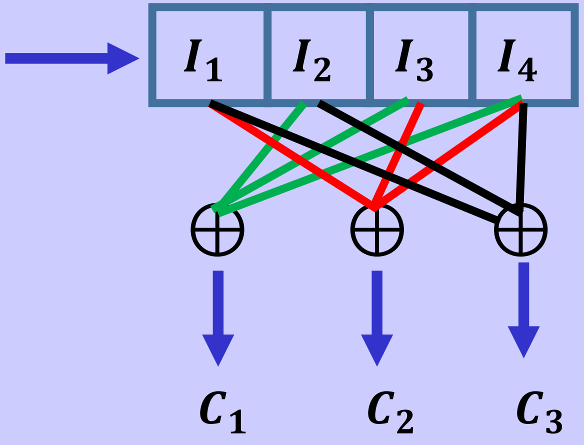
$$C = [1011].\begin{bmatrix} 1000011 \\ 0100101 \\ 0010110 \\ 0001111 \end{bmatrix}$$

$$C = [1011010]$$

$$C = [I_1 I_2 I_3 I_4 C_1 C_2 C_3]$$

$$C_1 = I_2 \oplus I_3 \oplus I_4$$
$$C_2 = I_1 \oplus I_3 \oplus I_4$$
$$C_3 = I_1 \oplus I_2 \oplus I_4$$

$C_1 = I_2 \oplus I_3 \oplus I_4$
$C_2 = I_1 \oplus I_3 \oplus I_4$
$C_3 = I_1 \oplus I_2 \oplus I_4$



Codeword Truth Table:

Data 4 bits $I_1I_2I_3I_4$	Codeword 7 bits $I_1I_2I_3I_4C_1C_2C_3$
0000	0000000
0001	0001111
0010	0010
0011	0011
….	….
….	….
1111	1111

If codeword [0011001] find received signal

$$H = [P^T_{rxk} : I_{rxr}]$$

$$H = \begin{bmatrix} 0111100 \\ 1011010 \\ 1101001 \end{bmatrix}$$

$$H.C^T = \begin{bmatrix} 0111100 \\ 1011010 \\ 1101001 \end{bmatrix} . \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

It is correct codeword datat is [0011]

If codeword [0010001] find received signal

$$H.C^T = \begin{bmatrix} 0111100 \\ 1011010 \\ 1101001 \end{bmatrix} . \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

There is error [0010001] correct codeword [0011001]

Homework 4: The generator matrix of a LBC is given by:

$$[G] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

a-Use Hamming bound to find error correction capability. b-Find the parity check matrix. c-find the code table, Hamming weight and the error correction capability then compare with part(a). d-If the received word is [R]=[1011110011], find the corrected word at the Rx.

Cyclic Codes

These are subclass from the linear block codes. The name cyclic comes from the fact that any cyclic shift of a codeword is another codeword. i.e, if [C1]=[0011010] is a codeword then [C2]=[0001101] is another codeword obtained from [C1] by a right circular shift.

Cyclic codes can be classified into two types:

- Nonsystematic cyclic codes
- Systematic cyclic codes

Generation of cyclic codes:

A) nonsystematic Cyclic Codes: (Multiplicative):

Procedure:

(1) For [D]=[a_1 a_2 ….. a_k] data word, write the data word in terms of a power of a dummy variable x with a_1 weighted as MSB (Most Significant Bit) and a_k as LSB(Least Significant Bit).

x^{k-1}	x^{k-2}		x^2	x^1	x^0
a_1	a_2	…….	a_{k-2}	a_{k-1}	a_k
MSB					LSB

$D(x)=a_k+a_{k-1}x+a_{k-2}x^2+\ldots\ldots+a_2x^{k-2}+a_1x^{k-1}$ where "+" sign is mod-2 addition(Ex-OR)

For example if [D]=[1 1 1 0 1],

then $D(x)=1+x^2+x^3+x^4$

and if $D(x)=x^6+x^2+1$ then [D]=[1000101]

2) Multiply D(x) by what is called generator polynomial g(x) of order r=n-k.

(3) The output codeword polynomial will be:

$C(x)=D(x)\,g(x)$ from which we can find the output codeword [C]

Example: $g(x) = x^3 + x + 1$

A.

1. $x^r = x^3$
2. have x^r , 1

B.

D=[1 0 1 1]

MSB LSB

$$D(x) = 1 + 1x + 0x^2 + 1x^3$$
$$D(x) = 1 + 1x + 1x^3$$

D=[1 0 0 0]

$$D(x) = x^3$$

Example 10: Find codeword using nonsystematic cyclic code, if $g(x) = x^3 + x + 1$and $D = [\,0\ 0\ 1\ 1]$

Solution:

1. $G(x) = x^3 + x + 1$

   r=3

2. $D = [\,0\ 0\ 1\ 1]$

   $D(\mathrm{x}) = 1 + x$ ===> k=4

$N = k + r = 4 + 3 = 7$

Code (7,4) , code rate = 4/7

$$C(x) = G(x)D(x)$$

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

$$=\left[x^4 + x^2 + x + x^3 + x + 1\right]$$

$$C(x) = [0011101]$$

Homework 5: Find codeword using nonsystematic cyclic code, if $g(x) = x^4 + x^2 + 1$and $D = [\,1001]$