CHAPTER7

CODING THEORY

Coding Theory

- In digital communications, when information is transmitted in the form of strings of 0's and 1's, certain problems arise.

- As a result of "**noise**" in the channel, when a certain signal is transmitted a different signal may be received, thus causing the receiver to make a wrong decision.

Coding Theory

- Hence we want to develop techniques to help us detect, and perhaps even correct transmission errors.

- However, we can only improve the chances of correct transmission; there are no guarantees.

Coding of Binary Information

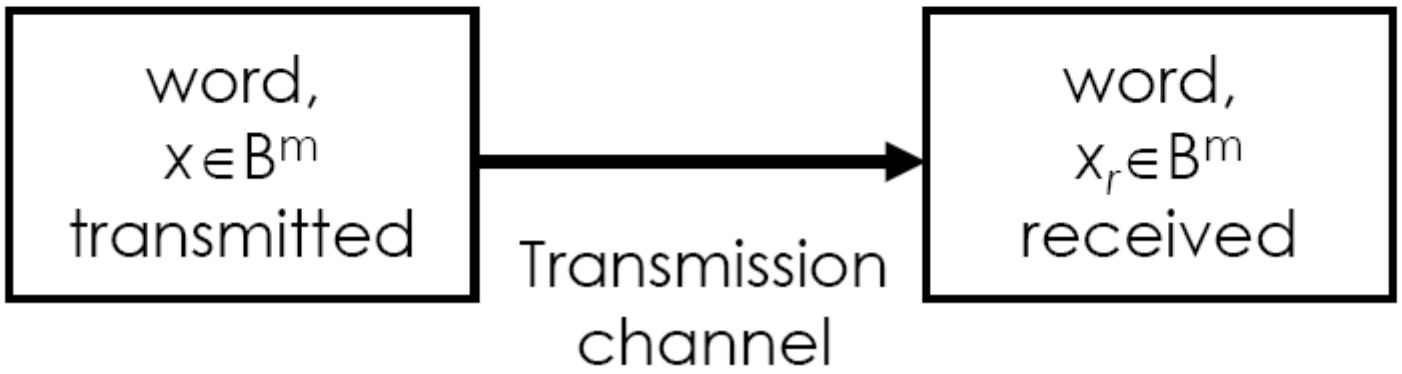
- The basic unit of information, called a message, is a finite sequence of characters from a finite alphabet.

- We shall choose our alphabet as the set B={0, 1}

Coding of Binary Information

- Every character or symbol that we want to transmit is now represented as a sequence of **m** elements from **B={0,1}.**
- That is, every character or symbol is represented in binary form.
- Our basic unit of information, called a word, is a sequence of **m** **0**'s and **1**'s.

Coding of Binary Information



Coding of Binary Information

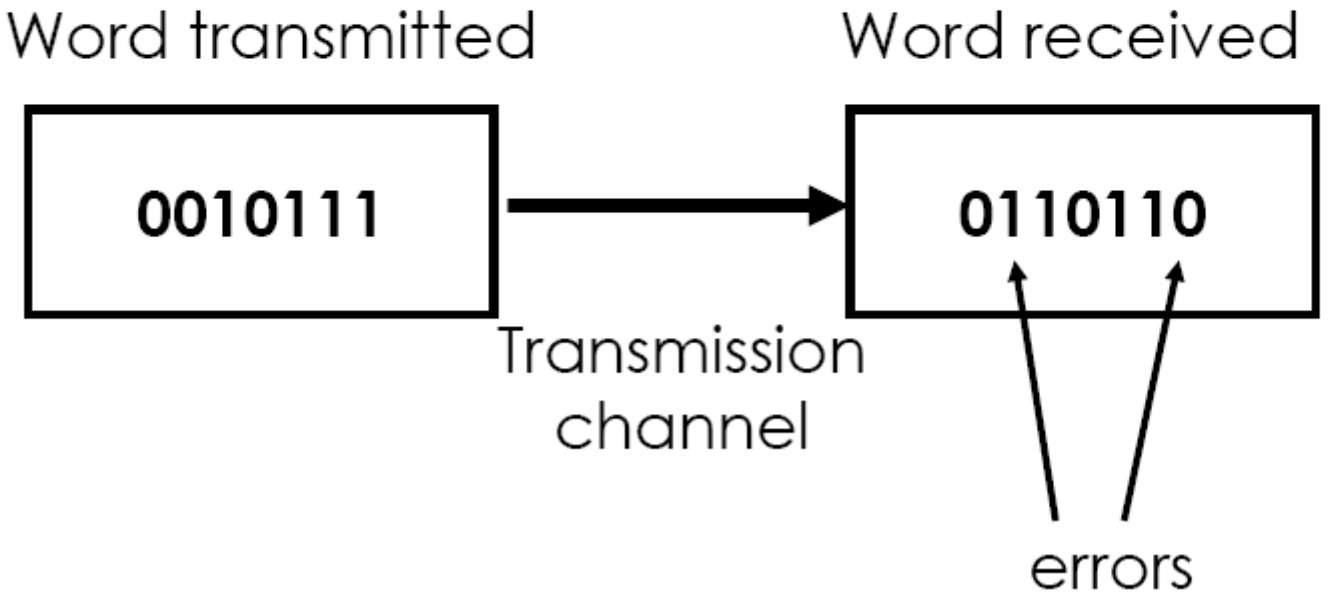
- In actual practice, the transmission channel may suffer disturbances which are generally called noise, due to weather interference, electrical problems, and so on.

- That may cause a 0 to be received as a 1, or vice versa.

Coding of Binary Information

- This erroneous transmission of digits in word being sent may give rise to the situation where the word received is different from the word that was sent.

example


Word transmitted
Word received
0010111
0110110
Transmission channel
errors

Coding of Binary Information

- The basic task in the transmission is to reduce the likelihood of receiving a word that differs from the word was sent.

- This is done as follows.

Coding of Binary Information

- Choose an integer n>m and one-to-one function f: $B^m \rightarrow B^n$.
- The function f is called an (m,n) encoding function.

  (representing every word in B^m as a word in B^n)

example

- Consider the following (m,3m) encoding function f: $B^m \rightarrow B^{3m}$ if

$$b = b_1 b_2 \ldots b_m \in B^m$$

- Define

$$f(b) = f(b_1 b_2 \ldots b_m)$$
$$= b_1 b_2 \ldots b_m \, b_1 b_2 \ldots b_m \, b_1 b_2 \ldots b_m$$

example

- Let m=3,

- Thus,

  f(100)=100100100

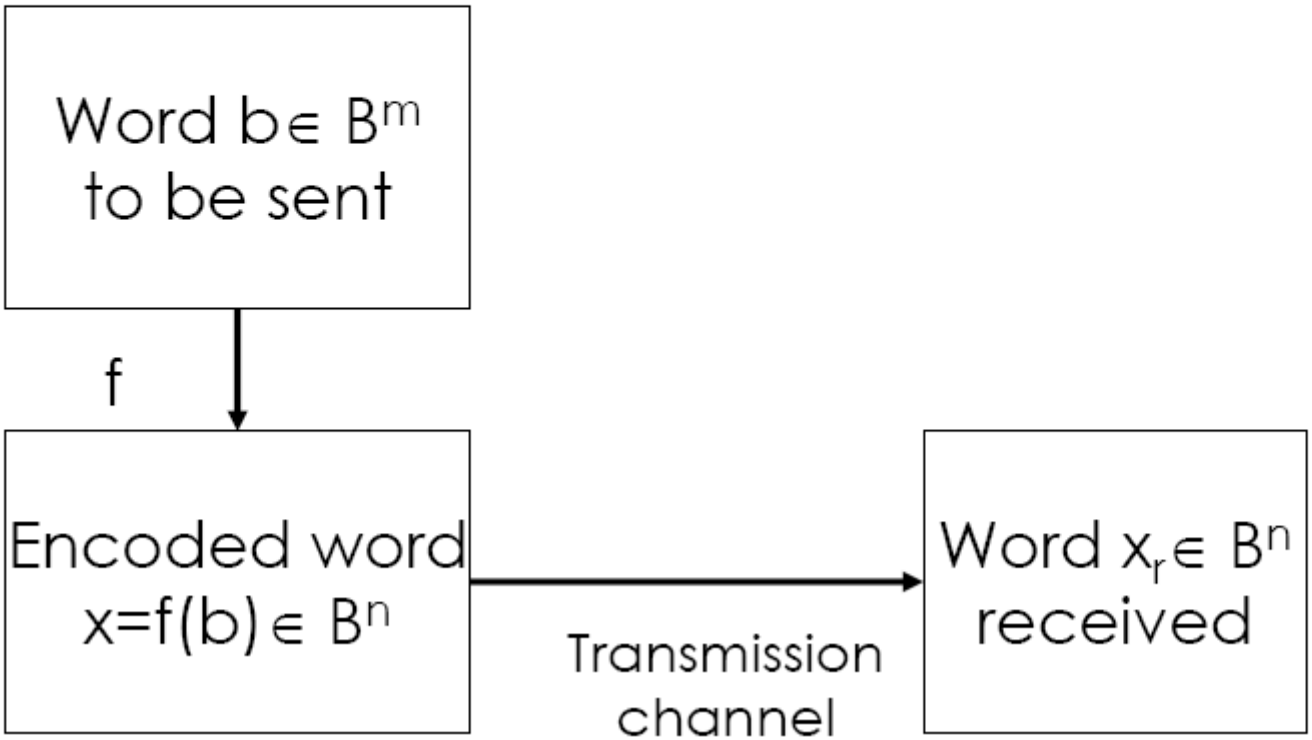
  f(011)=011011011

  f(001)=001001001

Coding of Binary Information

- If $b \in B^m$, then f(b) is called the code word representing b.
- The additional 0's and 1's can provide the means to detect or correct errors produced in the transmission channel.

Coding of Binary Information



Coding of Binary Information

- If the transmission channel is noiseless, then $x_r = x$ for all x in B^n.

- In this case $x=f(b)$ is received for each $b \in B^m$, and since f is a known function, b may be identified.

Error detection

- In general, errors in transmission do occur.
- The code word x=f(b) has been transmitted with k or fewer errors if x and x_r differ in at least 1 but no more than k positions.

Error detection

- Let f: $B^m \rightarrow B^n$ be an (m,n) encoding function.
- We say that f detects k or fewer errors if whenever x=f(b) is transmitted with k or fewer errors, then x_r is not a code word.

Weight

- If $x \in B^n$, then the number of 1's in x is called the weight of x and is denoted by $|\mathbf{x}|$.

example

- Find the weight each of the following words in B^5

  i) 11000 = 2

  ii) 11111 = 5

  iii) 10101 = 3

  iv) 01010 = 2

exercise

- Find the weight each of the following words :
  i) 1000110
  ii) 0111001
  iii) 11110001
  iv) 10101010

Parity Check Code

- The encoding function f: $B^m \rightarrow B^{m+1}$ is called the parity (m, m+1) check code:

  if $b = b_1 b_2 \ldots b_m \in B^m$, define

$$f(b) = b_1 b_2 \ldots b_m \, b_{m+1}$$

where

$$b_{m+1} = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd} \end{cases}$$

Parity Check Code

- b_{m+1} is zero if and only if the number of 1's in b is an even number.
- Every code word f(b) has even weight.
- A single error in the transmission of a code word will change the received word to a word of odd weight, and therefore can be detected.

example

- Let m=3.
  - f(001) = 001**1**
  - f(110) = 110**0**
  - f(111) = 111**1**
  - f(101) = 101**0**

exercise

- Consider the (3,4) parity check code. For each of received words, determine whether an error will be detected.
  - 0100
  - 1100
  - 0010
  - 1001

Hamming Distance

- Let x and y be words in B^m.
- The Hamming distance, **H(x,y)** between x and y is the weight $|\mathbf{x} \oplus \mathbf{y}|$ of $\mathbf{x} \oplus \mathbf{y}$.

Hamming Distance

- $x \oplus y$

$x \oplus y$	x=0	x=1
y=0	0	1
y=1	1	0

example

- Find the distance between x and y:

x=110110, y=000101
x=011101, y=100101
x=01011, y=11001

example

x=110110, y=000101

$110110 \oplus 000101 = 110011$

$$\begin{array}{r} 110110 \\ 000101 \\ \hline 110011 \end{array}$$

$|110011| = 4$

example

x= 011101, y= 100101

$011101 \oplus 100101 = 111000$

$$\begin{array}{r} 011101 \\ 100101 \\ \hline 111000 \end{array}$$

$|111000| = 3$

example

x=01011, y=11001

$01011 \oplus 11001 = 10010$

01011
11001
10010

$|10010| = 2$

Properties of the distance function

- Let x, y and z be elements of B^m. Then
  - $H(x, y) \geq 0$
  - $H(x, y) = 0$ if and only if $x=y$
  - $H(x, y) = H(y, x)$
  - $H(x, y) + H(y, z) \geq H(x, z)$

Minimum Distance

- The minimum distance of an encoding function f: $B^m \rightarrow B^n$ is the minimum of the distances between all distinct pairs of code words.

$$\min \{ H(f(x), f(y)) \mid x, y \in B^m \}$$

example

- Find the minimum distance of the (2,5) encoding function f:

f(00) = 00000
f(10) = 00111
f(01) = 01110
f(11) = 11111

example

- 6 distinct pairs of code words:

f(00),f(10)	f(00),f(01)	f(00),f(11)
f(10),f(01)	f(10),f(11)	f(01),f(11)

- Compute the distance for each pair.

example

$$|f(00) \oplus f(10)| = |00000 \oplus 00111|$$
$$= |00111| = 3$$

$$|f(00) \oplus f(01)| = |00000 \oplus 01110|$$
$$= |01110| = 3$$

$$|f(00) \oplus f(11)| = |00000 \oplus 11111|$$
$$= |11111| = 5$$

example

$$|f(10) \oplus f(01)| = |00111 \oplus 01110|$$
$$= |01001| = 2$$

$$|f(10) \oplus f(11)| = |00111 \oplus 11111|$$
$$= |11000| = 2$$

$$|f(01) \oplus f(11)| = |01110 \oplus 11111|$$
$$= |10001| = 2$$

example

- Hamming distance,

  3, 3, 5, 2, 2, 2

  Minimum 2

- The minimum distance is 2.

Theorem

- An (m,n) encoding function f: $B^m \rightarrow B^n$ can detect k or fewer errors if and only if its minimum distance is at least k+1.

example

- Consider the (2,5) encoding function

  f: $B^2 \rightarrow B^5$:

  f(00) = 00000

  f(10) = 00111

  f(01) = 01110

  f(11) = 11111

- How many errors will f detect?

example

- The minimum distance of f is 2.
- The code k or fewer errors if and only if its minimum distance is at least k+1.
- $2 \geq k+1$ or $k \leq 1$
- The code can detect 1 error.

exercise

- Consider the (2,5) encoding function

  f: $B^2 \rightarrow B^5$

  f(00) = 00000

  f(01) = 01110

  f(10) = 10101

  f(11) = 11011

- How many errors will f detect?

Exercise
Past Year 2015/2016

a) Let C be the set of code words {00000000, 11111000, 01010111, 10101111}. How many errors can C detect? (6 marks)

Group Codes

- An encoding function $f : B^m \rightarrow B^n$ is called a group code if

$$f(B^m) = \{ f(b) \mid b \in B^m \}$$

is a subgroup of B^n.

Group Codes

- **N** is a subgroup of B^n if:
  - The identity i of B^n is in N.
    x ⊕ i=x, **i ⊕ x=x,** $x \in B^n$, $x \in N$

Group Codes

- if x and y $\in$ N, then x $\oplus$ y $\in$ N.
- if x $\in$ N, then $x^{-1} \in$ N.

  $\mathbf{x \oplus x^{-1}=i}$, $\mathbf{x^{-1} \oplus x=i}$

  (need not be checked, since every element in B^n is its own inverse)

example

- Show that the encoding function $f : B^2 \rightarrow B^5$ is a group code.

f (00) = 00000
f (01) = 01110
f (10) = 10101
f (11) = 11011

example

- We must show that the set of all code words

  N={00000, 01110, 10101, 11011}

  is a subgroup of B^5.

example

Let

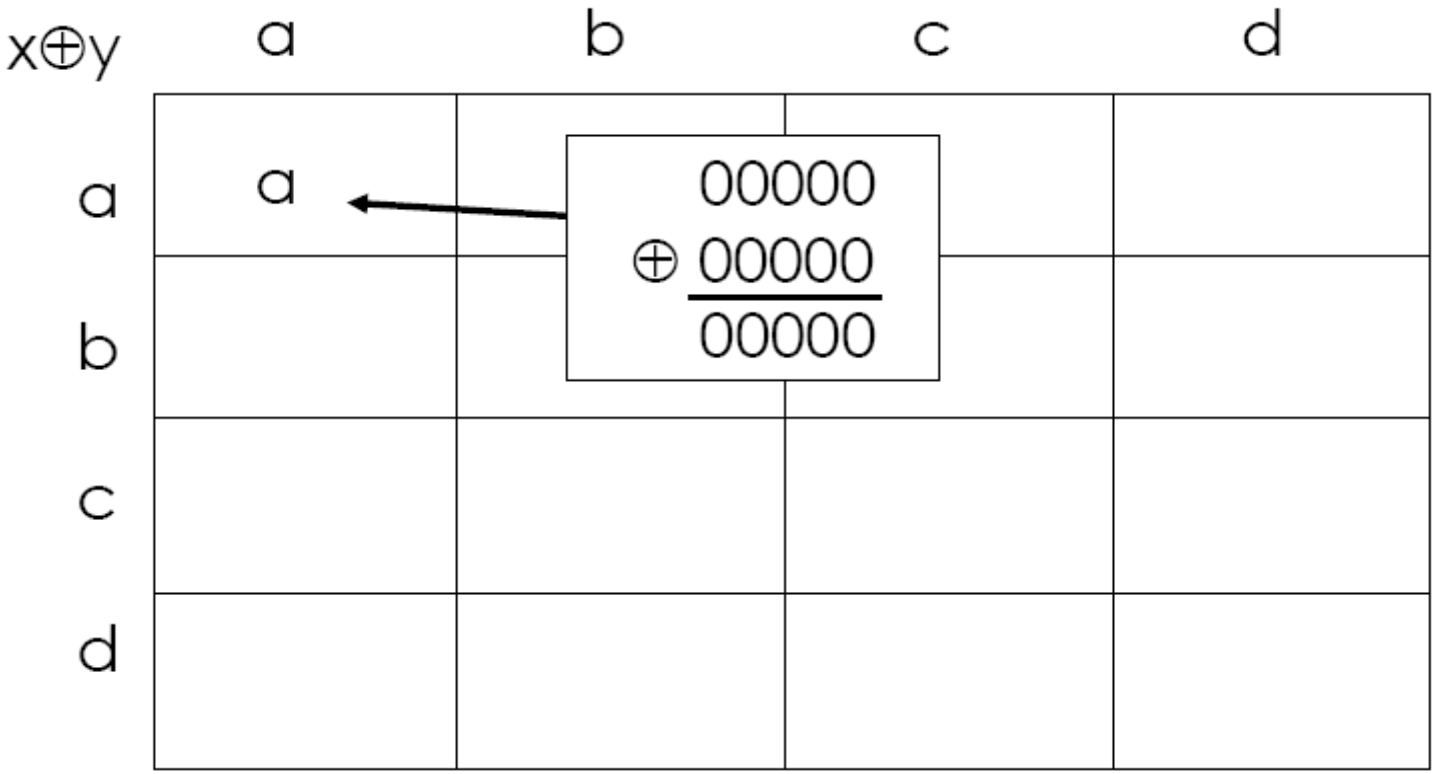
a=00000

b=01110

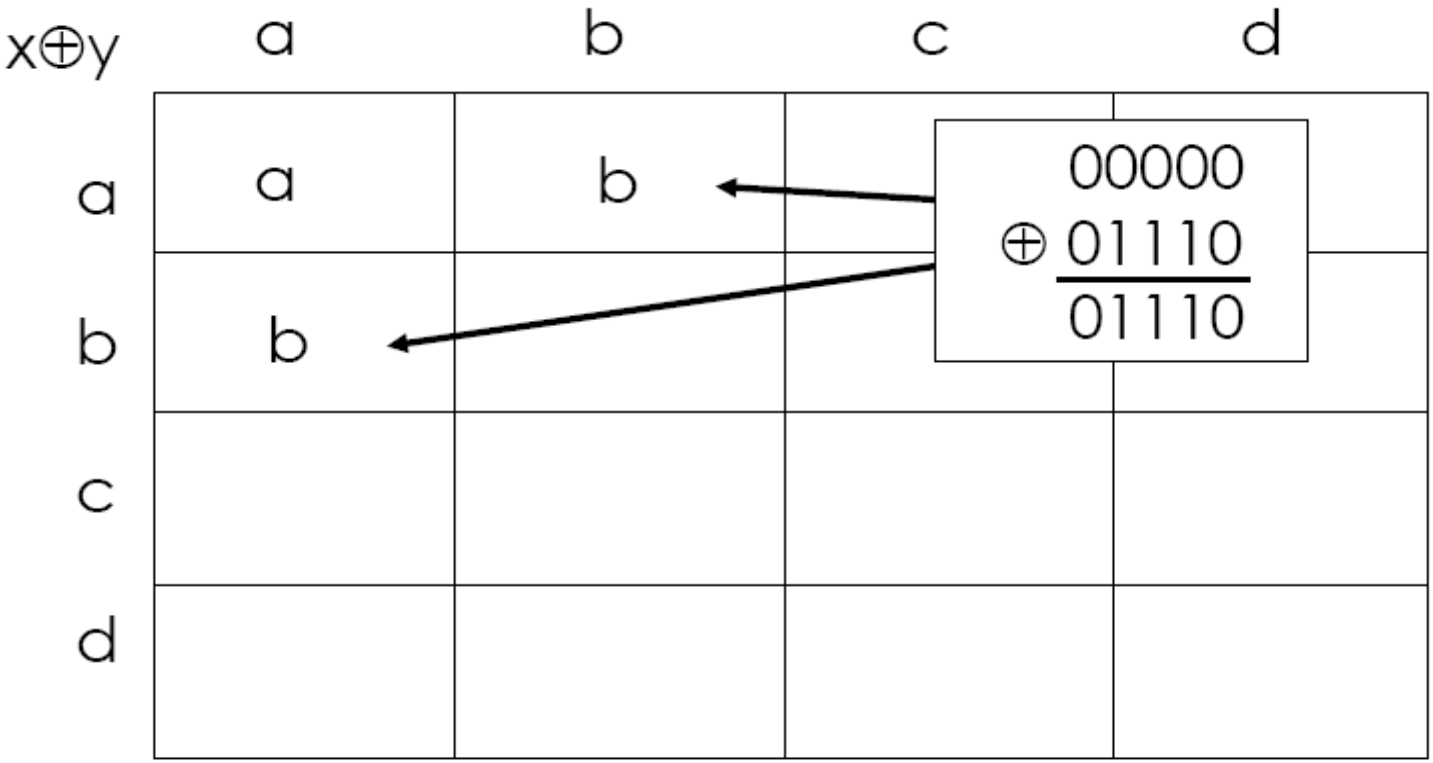
c=10101

d=11011

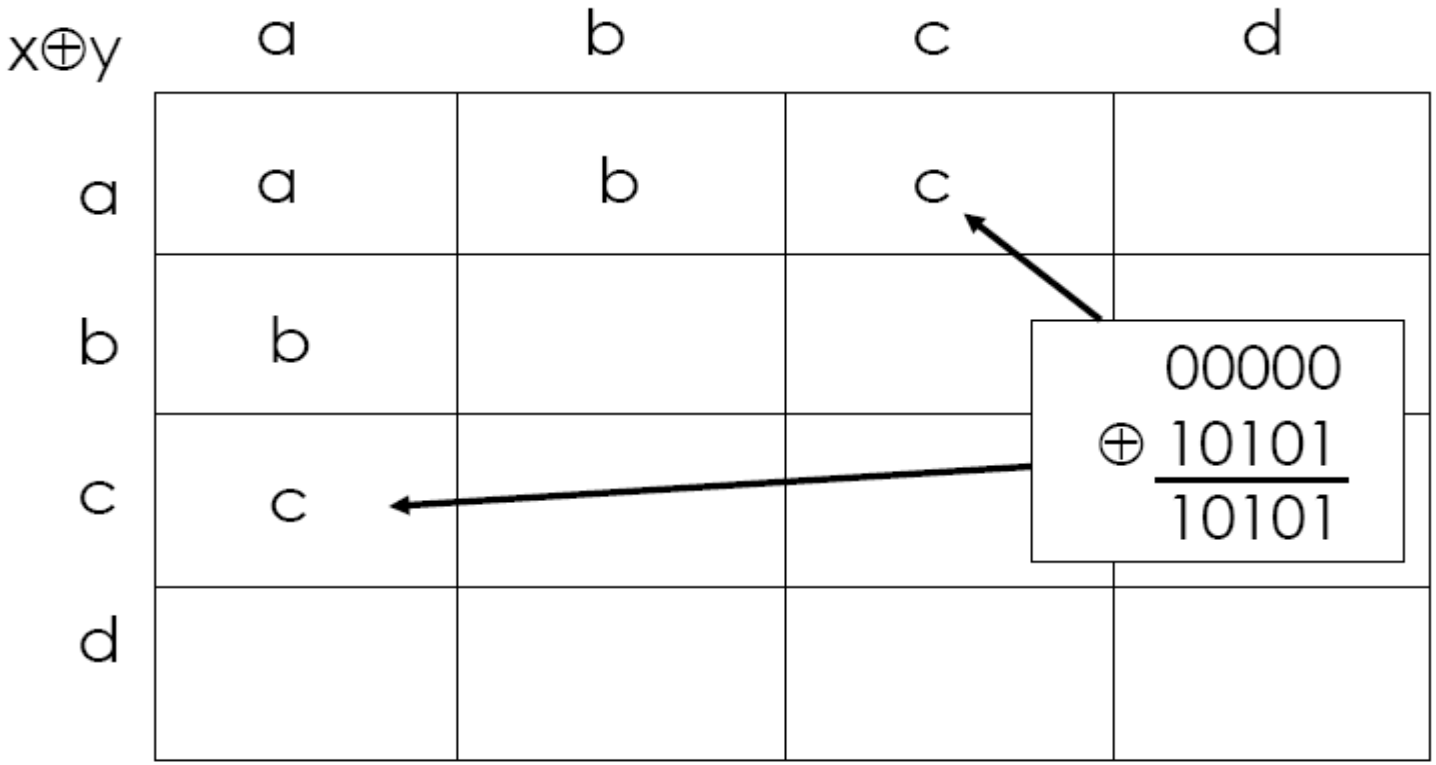
a=00000, b=01110, c=10101, d=11011



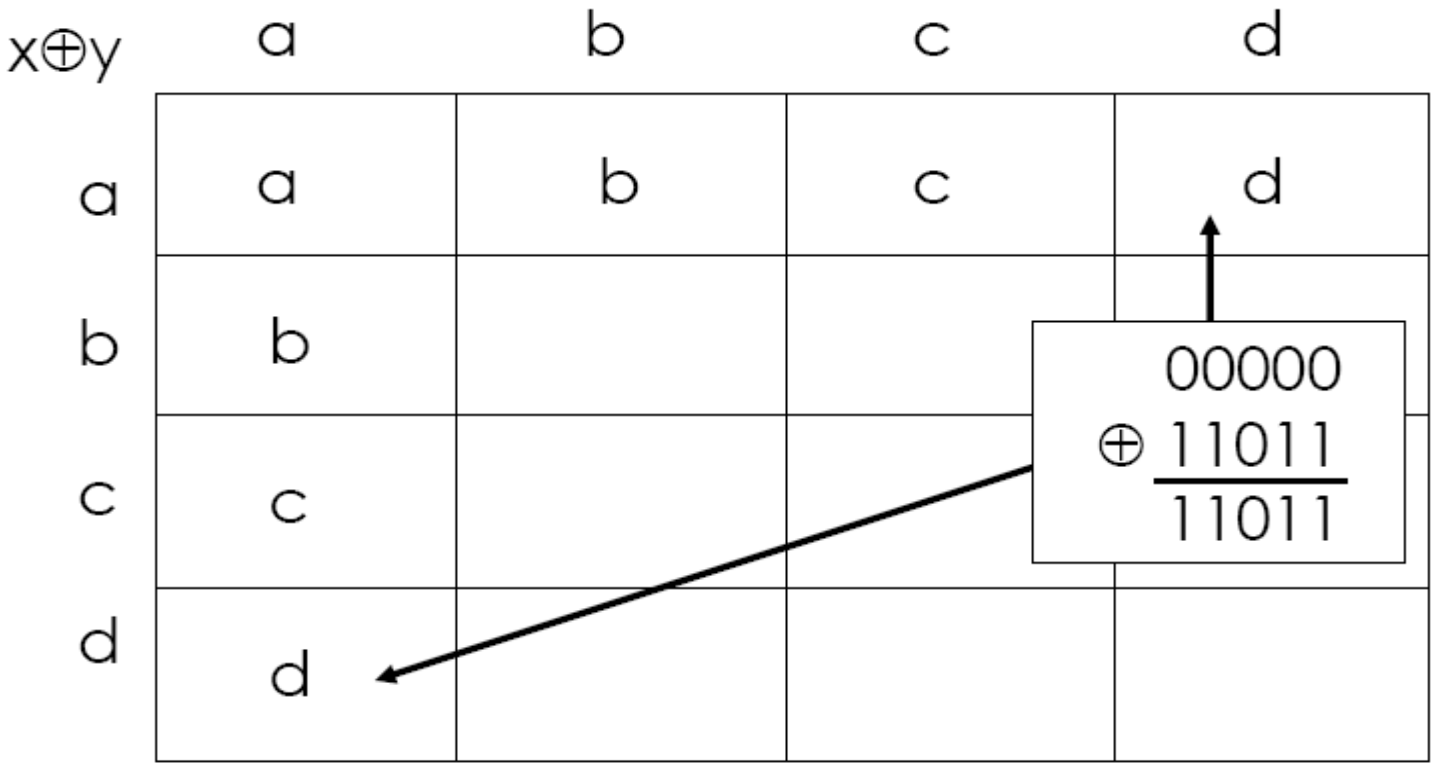
a=00000, b=01110, c=10101, d=11011



a=00000, b=01110, c=10101, d=11011



a=00000, b=01110, c=10101, d=11011



a=00000, b=01110, c=10101, d=11011

x⊕y	a	b	c	d
a	a	b	c	d
b	b	a		
c	c			
d	d			

$$\begin{array}{r} 01110 \\ \oplus\ 01110 \\ \hline 00000 \end{array}$$

a=00000, b=01110, c=10101, d=11011

x⊕y	a	b	c	d
a	a	b	c	d
b	b	a	d	
c	c	d		
d	d			

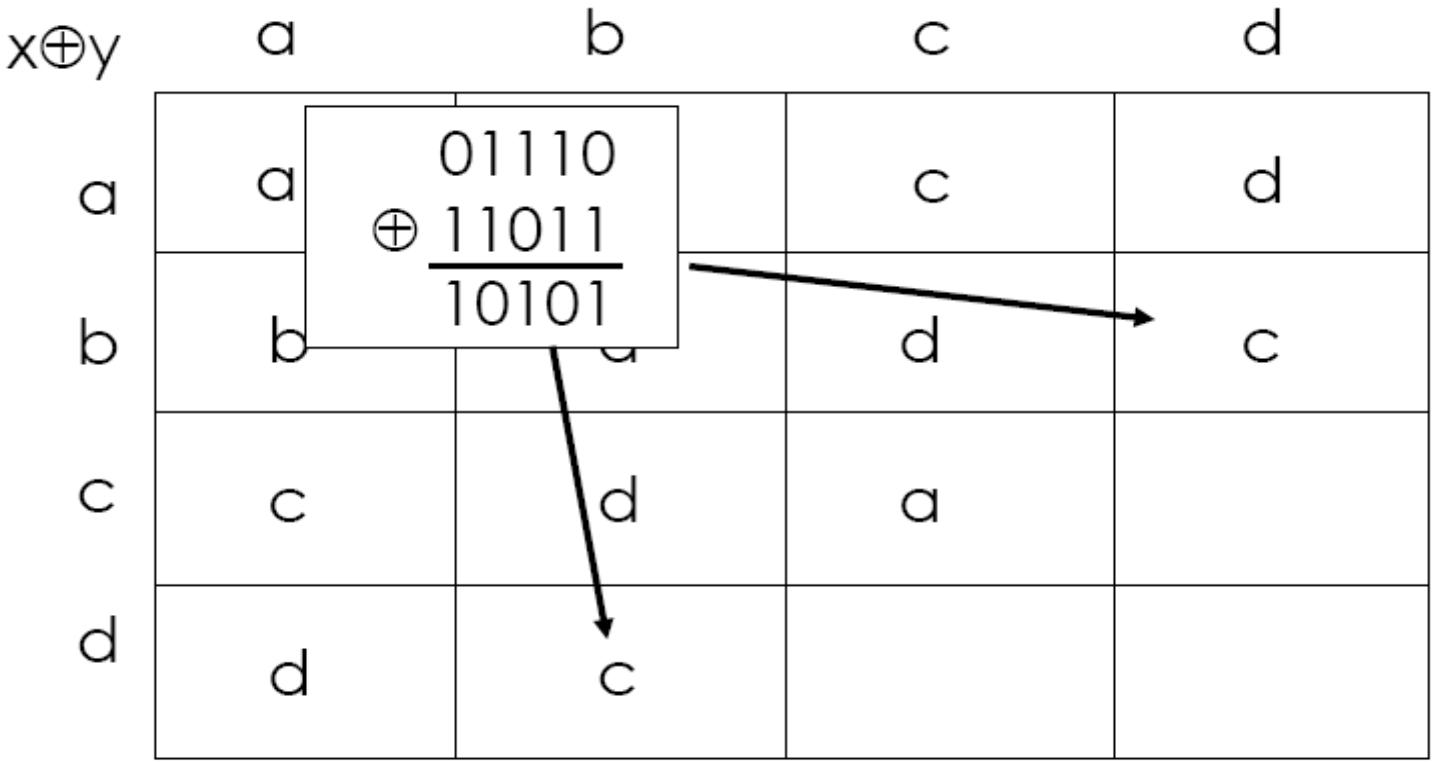
$$\begin{array}{r} 01110 \\ \oplus\ 10101 \\ \hline 11011 \end{array}$$

a=00000, b=01110, c=10101, d=11011

x⊕y	a	b	c	d
a	a		c	d
b	b		d	
c	c	d	a	
d	d			

$$\begin{array}{r} 10101 \\ \oplus\ 10101 \\ \hline 00000 \end{array}$$

a=00000, b=01110, c=10101, d=11011



a=00000, b=01110, c=10101, d=11011

x⊕y	a	b	c	d
a	a		c	d
b	b		d	c
c	c	d	a	b
d	d	c	b	

$$\begin{array}{r} 10101 \\ \oplus\ 11011 \\ \hline 01110 \end{array}$$

a=00000, b=01110, c=10101, d=11011

x⊕y	a	b	c	d
a	a	b	c	d
b	b	11011 ⊕ 11011 = 00000	d	c
c	c	d	a	b
d	d	c	b	a

a=00000, b=01110, c=10101, d=11011

$x \oplus y$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

example

- The identity of B^n belongs to N

  $i = 00000 = a$

- $x, y \in N, \; x \oplus y \in N$

- The encoding function f is a group code.

exercise

- Show that the encoding function $f : B^3 \rightarrow B^7$ is a group code.

f (000)=0000000 f (001)=0010110
f (010)=0101000 f (011)=0111110
f (100)=1000101 f (101)=1010011
f (110)=1101101 f (111)=1111011

Group Codes

- Let D=[d_{ij}] and E=[e_{ij}] be m×n Boolean matrices.

- We define the **mod 2 sum** D⊕E as the m×n Boolean matrix F=[f_{ij}] where

  - $f_{ij} = d_{ij} + e_{ij}$

example

$$\text{Let } D = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad E = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

example

- D⊕E

$$\begin{bmatrix} \boxed{1} & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} \boxed{1} & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \boxed{1+1} & 0+1 & 1+0 & 1+1 \\ 0+1 & 1+1 & 1+0 & 0+1 \\ 1+0 & 0+1 & 0+1 & 1+1 \end{bmatrix} = \begin{bmatrix} \boxed{0} & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Group Codes

- Let D=[d_{ij}] be an m×p Boolean matrix and let E=[e_{ij}] be a p×n Boolean matrix.

- We define the **mod 2 Boolean product** D*E as the m×n matrix F=[f_{ij}] where

  - $f_{ij} = d_{i1}.e_{1j} + + d_{i2}.e_{2j} .. + d_{ip}.e_{pj}$

example

$$\text{Let } D = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \qquad E = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

example

- D*E

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1.1+1.1+0.0 & 1.0+1.1+0.1 \\ 0.1+1.1+1.0 & 0.0+1.1+1.1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Group Codes

- Let m < n and r=n–m. An n×r Boolean matrix, **H**

  whose last r rows form the identity matrix, is called a **parity check matrix**.

$$H = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1r} \\ h_{21} & h_{22} & \dots & h_{2r} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \dots & h_{mr} \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} r = n - m$$

Group Codes

- We use H to define an encoding function $f_H: B^m \rightarrow B^n$
- If $b = b_1 b_2 \ldots b_m$,
- Let $x = f_H(b)$

Group Codes

$f_H(b) = b_1 b_2 \ldots b_m x_1 x_2 \ldots x_r$

where,

$$[b_1 \quad b_2 \quad \ldots \quad b_m] * \begin{bmatrix} h_{11} & h_{12} & \ldots & h_{1r} \\ h_{21} & h_{22} & \ldots & h_{2r} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \ldots & h_{mr} \end{bmatrix}$$

$$= [x_1 \quad x_2 \quad \ldots \quad x_r]$$

example

- Let m=2, n=5 and

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

- Determine the group code $f_H: B^2 \rightarrow B^5$

example

- We have B^2 ={ 00, 01, 10, 11 }
- b= b_1b_2 and x= $f_H(b)$= b_1b_2 x_1x_2 x_3

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$[b_1 \quad b_2] * \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [x_1 \quad x_2 \quad x_3]$$

example

- $f_H(00) = 00\ x_1x_2\ x_3$
- b= 00

$$[0 \quad 0]*\begin{bmatrix}1 & 0 & 1\\ 1 & 1 & 1\end{bmatrix}$$
$$=[0.1+0.1 \quad 0.0+0.1 \quad 0.1+0.1]$$
$$=[0 \quad 0 \quad 0]$$

- $f_H(00) = 00000$

example

- $f_H(01) = 01\ x_1x_2\ x_3$
- b= 01

$$[0 \quad 1] * \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$= [0.1+1.1 \quad 0.0+1.1 \quad 0.1+1.1]$$

$$= [1 \quad 1 \quad 1]$$

- $f_H(01) = 01111$

example

- $f_H(10) = 10\, x_1 x_2\, x_3$
- b= 10

$$\begin{bmatrix}1 & 0\end{bmatrix} * \begin{bmatrix}1 & 0 & 1\\ 1 & 1 & 1\end{bmatrix}$$

$$= \begin{bmatrix}1.1+0.1 & 1.0+0.1 & 1.1+0.1\end{bmatrix}$$

$$= \begin{bmatrix}1 & 0 & 1\end{bmatrix}$$

$f_H(10)$= 10101

- $f_H(01)$= 10101

example

- $f_H(11) = 11\ x_1x_2\ x_3$
- b= 11

$$[1 \quad 1]*\begin{bmatrix}1 & 0 & 1\\ 1 & 1 & 1\end{bmatrix}$$

$$=[1.1+1.1 \quad 1.0+1.1 \quad 1.1+1.1]$$

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

- $f_H(11) = 11010$

exercise

- Let,

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Determine the group code $f_H: B^2 \rightarrow B^5$

b) Suppose the encoding function be $f_H : B^4 \rightarrow B^7$ and the parity check matrix, H is given by

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Determine the code words representing word **1110** and **1011**. (4 marks)

Decoding and Error Correction

- Consider an (m,n) encoding function $f:B^m \rightarrow B^n$.
- The encoded word, $x=f(b) \in B^n$, for $b \in B^m$, is received as the word x_r
- we are faced with the problem of identifying the word b that was the original message.

Decoding and Error Correction

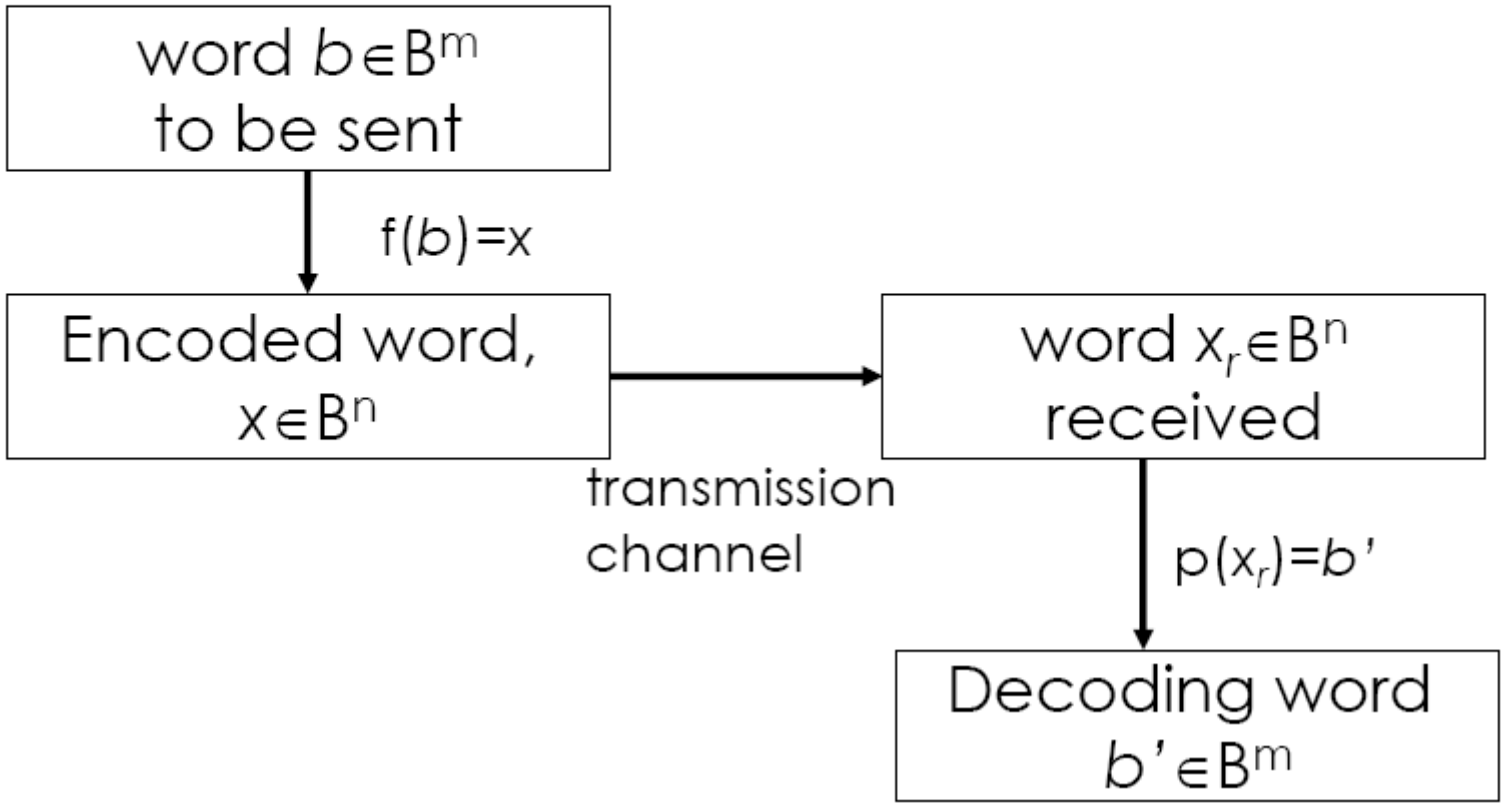
- An onto function **p: $B^n \rightarrow B^m$** is called an (n,m) decoding function associated with f, if

$$p(x_r) = b'$$

such that when the transmission channel has no noise then

$$b' = b$$

Decoding and Error Correction



Decoding and Error Correction

- The decoding function **p** is required to be **onto** so that every received word can be decoded to give a word in B^m.

- It decodes properly received words correctly, but decoding of improperly received words may or may not be correct.

example

- The parity check code, f: $B^m \rightarrow B^{m+1}$.

- The decoding function, p: $B^{m+1} \rightarrow B^m$

  If $y = y_1 y_2 \ldots y_m y_{m+1} \in B^{m+1}$,

  then $p(y) = y_1 y_2 \ldots y_m \in B^m$

- Let m=4,

  p(10010)=1001 p(10001)=1000

Decoding and Error Correction

- Let f be an (m,n) encoding function
- Let p be an (n,m) decoding function associated with f.

Decoding and Error Correction

- The pair (f,p) correct k or fewer errors if whenever x=f(b) is transmitted correctly or with k or fewer errors and x_r is received, then $p(x_r)=b$

- Thus x_r is decoded as the correct message b.

Decoding and Error Correction

- Given an (m,n) encoding function,

  $f: B^m \rightarrow B^n$

- We often need to determine an (m,n) decoding function,

  $p: B^n \rightarrow B^m$

  associated with f.

Decoding and Error Correction

- We now discuss a method, called the **maximum likelihood technique**, for determining a decoding function p for a given f.

Decoding and Error Correction

- Since B^m has m elements, there are 2^m code words in B^n.
- List the code words in a fixed order:

$$x^{(1)}, x^{(2)}, \ldots\ldots, x^{(2^m)}$$

Decoding and Error Correction

- If the received word is x_r, we compute,

  $H(x^{(i)}, x_r)$ for $1 \le i \le 2^m$

and choose the first code word, say it is $x^{(s)}$, such that

$$\min_{1 \le i \le 2^m} \{H(x^{(i)}, x_t)\} = x^{(s)}$$

Decoding and Error Correction

- $x^{(s)}$ is a code word that is closest to x_r, and the first in the list.

- If $x^{(s)} = f(b)$, we define the maximum likelihood decoding function p associated with f by

$$p(x_r) = b$$

Decoding and Error Correction

- p depends on the particular order in which code words in $f(B^m)$ are listed.

- If the code words are listed in a different order, we may obtain a different maximum likelihood decoding function p associated with f.

Decoding Procedure

- If f: $B^m \rightarrow B^n$ is a group code, the procedure for obtaining a maximum likelihood decoding function associated with f:

1. Determine all the left cosets of $N=f(B^m)$ in B^n.

2. For each coset, find a coset leader (a word of least weight)

Decoding Procedure

3. If the word x_r is received, determine the coset of N to which x_r belongs. There are $2^n/2^m$ distinct cosets of N in B^n.

4. Let e be a coset leader for the coset determined in (3).

   Compute, $x = x_r \oplus e$

   if $x=f(b)$, we let $p(x_r)=b$.

   That is, we decode x_r as b.

Decoding Procedure

- Keep a complete list of all cosets of N in tabular form.
- Each row of the table containing one coset.
- Identify a coset leader in each row.

Decoding Procedure

- When a word x_r is received, we locate the row which contains it, find the coset leader for that row, and add it to x_r.

- This gives us the code word closest to x_r.

Decoding Procedure

- Let $N = \{x^{(1)}, x^{(2)}, ..., x^{(2^m)}\}$

  where $x^{(1)}$ is $\overline{0}$ the identity of B^n.

- List all the elements of N in a row, starting with identity at the left

$$\overline{0} \quad x^{(2)} \quad x^{(2)} \quad .... \quad x^{(2^m)}$$

coset leader, e_1

Decoding Procedure

- Choose any word (least weight) e_2 in B^n which has not been listed in the first row.

- List the elements of the coset $e_2 \oplus N$ as the second row.

$$e_2 \quad e_2 \oplus x^{(2)} \quad e_2 \oplus x^{(2)} \quad .... \quad e_2 \oplus x^{(2^m)}$$

coset leader

Decoding Procedure

- Choose another element (least weight) e_3 in B^n which has not been listed in either of the first two rows and form the third row.

$$e_3 \quad e_3 \oplus x^{(2)} \quad e_3 \oplus x^{(2)} \quad \ldots \quad e_3 \oplus x^{(2^m)}$$

coset leader

- Continue this process until all elements of B^n have been listed.

example

- Consider the (3,5) encoding function defined by

f(000)=00000	f(100)=10011
f(001)=00110	f(101)=10101
f(010)=01001	f(110)=11010
f(011)=01111	f(111)=11100

example

- Decode the following words relative to a maximum likelihood decoding function:
  - 11001
  - 01010
  - 00111

example

- N = { 00000, 00110, 01001, 01111, 10011, 10101, 11010, 11100 }

$$= \{x^{(1)}, x^{(2)}, \ldots\ldots, x^{(2^m)}\}$$

- $2^5/2^3 = 2^2 = 4$ cosets (4 rows)

example

- Coset leader, e_1 the identity of B^n ($e_1 \in N$)
- e_1 =00000

example

- Row 1,

$e_1 = 00000$

$e_1 \oplus 00110 = 00110$

$e_1 \oplus 01001 = 01001$

$e_1 \oplus 01111 = 01111$

$e_1 \oplus 10011 = 10011$

$e_1 \oplus 10101 = 10101$

$e_1 \oplus 11010 = 11010$

$e_1 \oplus 11100 = 11100$

example

- Row 2, coset leader e_2=00001

$e_2 = 00001$

$e_2 \oplus 00110 = 00111$

$e_2 \oplus 01001 = 01000$

$e_2 \oplus 01111 = 01110$

$e_2 \oplus 10011 = 10010$

$e_2 \oplus 10101 = 10100$

$e_2 \oplus 11010 = 11011$

$e_2 \oplus 11100 = 11101$

example

- Row 3, coset leader e_3 =00010

$$
\begin{aligned}
e_3 &= 00010 \\
e_3 \oplus 00110 &= 00100 \\
e_3 \oplus 01001 &= 01011 \\
e_3 \oplus 01111 &= 01101 \\
e_3 \oplus 10011 &= 10001 \\
e_3 \oplus 10101 &= 10111 \\
e_3 \oplus 11010 &= 11000 \\
e_3 \oplus 11100 &= 11110
\end{aligned}
$$

example

- Row 4, coset leader e_4 =10000

$$
\begin{aligned}
e_4 &= 10000 \\
e_4 \oplus 00110 &= 10110 \\
e_4 \oplus 01001 &= 11001 \\
e_4 \oplus 01111 &= 11111 \\
e_4 \oplus 10011 &= 00011 \\
e_4 \oplus 10101 &= 00101 \\
e_4 \oplus 11010 &= 01010 \\
e_4 \oplus 11100 &= 01100
\end{aligned}
$$

example

00000	00110	01001	01111	10011	10101	11010	11100
00001	00111	01000	01110	10010	10100	11011	11101
00010	00100	01011	01101	10001	10111	11000	11110
10000	10110	11001	11111	00011	00101	01010	01100

Decode the following words relative to a maximum likelihood decoding function:

- 11001
- 01010
- 00111

example

00000	00110	01001	01111	10011	10101	11010	11100
00001	00111	01000	01110	10010	10100	11011	11101
00010	00100	01011	01101	10001	10111	11000	11110
10000	10110	11001	11111	00011	00101	01010	01100

- 11001 Column 3, 11001 ⊕ 10000 = 01001

f(010)=01001, → p(11001)= **010**

example

00000	00110	01001	01111	10011	10101	11010	11100
00001	00111	01000	01110	10010	10100	11011	11101
00010	00100	01011	01101	10001	10111	11000	11110
10000	10110	11001	11111	00011	00101	01010	01100

- 01010

Column 7, **01010 ⊕ 10000 = 11010**

f(110)=11010, → p(01010)= **110**

example

00000	00110	01001	01111	10011	10101	11010	11100
00001	00111	01000	01110	10010	10100	11011	11101
00010	00100	01011	01101	10001	10111	11000	11110
10000	10110	11001	11111	00011	00101	01010	01100

- 00111 Column 2, 00111 ⊕ 00001 = 00110

f(001)= 00110, → p(00111)= **001**

exercise

Consider the (3,6) encoding function defined by

f (000)=000000 f (001)=000110
f (010)=010010 f (011)=010100
f (100)=100101 f (101)=100011
f (110)=110111 f (111)=110001

Decode the following words:

(a) 011110 (b) 101011 (c) 110010

Theorem

- Suppose that f is an (m,n) encoding function and p is a maximum likelihood decoding function associated with f.

- Then (f,p) **can correct k or fewer errors** if and only if the minimum distance of f is at least **2k+1**.

example

- Let f be the (3,8) encoding function defined by

  f(000)=00000000 f(100)=10100100

  f(001)=10111000 f(101)=10001001

  f(010)=00101101 f(110)=00011100

  f(011)=10010101 f(111)=00110001

- Let p be an (8,3) maximum likelihood decoding function associated with f.
- How many errors can (f,p) correct?

example

- The minimum distance of f is 3, as can be checked by computing the minimum of the distances between all 28 distinct pairs of code words.

- Since the minimum distance of f is 3, we have

$$3 \geq 2k+1, \quad k \leq 1$$

- Thus (f,p) can correct 1 error.

exercise

- Given the following encoding function, f : B2→B5

  f (00) = 00000

  f (01) = 01010

  f (10) = 10111

  f (11) = 11110

- Let p be an (5,2) maximum likelihood decoding function associated with f.
- How many errors can (f,p) correct?

c) Let an encoding function, $f : B^2 \rightarrow B^5$, with f given by,

$$f(00) = 00000$$

$$f(01) = 01011$$

$$f(10) = 10110$$

$$f(11) = 11101$$

Decode the word **11110** and **10101** using the maximum likelihood method. (Note: Copy Table 6 in your answer booklet and complete the '?' cells). (10 marks)

Table 6

	$e_i \oplus 00000$	$e_i \oplus 01011$	$e_i \oplus 10101$	$e_i \oplus 11101$
$e_1 = 00000$	00000	01011	10101	11101
$e_2 = 10000$	10000	11011	00110	01100
$e_3 = ?$	?	?	?	?
$e_4 = 00100$	00100	01111	10010	11001
$e_5 = ?$	?	?	?	?
$e_6 = 00001$	00001	01010	10111	11100
$e_7 = ?$	?	?	?	?
$e_8 = 10100$	10100	10111	00010	01001