Decoding and Error Correction

译码与纠错

译码与纠错

Zhang Yanmei

ymzhang@bupt.edu.cn

College of Computer Science & Technology

Beijing University of Posts & Telecommunications

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

Decoding Function

- An onto function $d: B^n \to B^m$ is called an (n, m) *decoding function associated with e*(与e关联的译码函数) if $d(x_t) = b' \in B^m$ is such that when the transmission channel has no noise, then $b' = b$, that is,
  - $d \circ e = 1_{B^m}$， *where is the identity function on* B^m
- d is required to be *onto* so that every received word can be decoded to give a word in B^m.

Example (Parity check code)

- Define the decoding function $d: B^{m+1} \to B^m$.
  - If $y = y_1y_2\ldots y_my_{m+1} \in B^{m+1}$, then $d(y) = y_1y_2\ldots y_m$
- Observe that if $b = b_1b_2\ldots b_m \in B^m$, then
  - $(d \circ e)(b) = d(e(b)) = b$
  - so $d \circ e = 1_{Bm}$
- For a concrete example, let $m = 4$.
  - $d(10010) = 1001$
  - $d(11001) = 1100$

Example (Triple encoding)

- Consider the $(m, 3m)$ encoding function. Define the decoding function $d: B^{3m} \to B^m$.
- Let $y = y_1y_2\ldots y_my_{m+1}\ldots y_{2m}y_{2m+1}\ldots y_{3m}$, Then
  - $d(y) = z_1z_2\ldots z_m$
  - where

$$z_i = \begin{cases} 1 & \text{if } \{y_i, y_{i+m}, y_{i+2m}\} \text{ has at least two 1's} \\ 0 & \text{if } \{y_i, y_{i+m}, y_{i+2m}\} \text{ has less than two 1's} \end{cases}$$

  - E.g. $x_t = 011011111$, then $d(x_t) = 011$

Decoding function

- Let e be an (m, n) encoding function and let d be an (n, m) decoding function associated with e.
- The pair (e, d) is said to *correct k or fewer errors*
  - if whenever $x = e(b)$ is transmitted correctly or with k or fewer errors and x_t is received, then $d(x_t) = b$. Thus x_t is decoded as the correct message b.

Maximum likelihood technique – 极大似然技术

- Since B^m has 2^m elements, there are 2^m code words in B^n. List it as $x^{(1)}, x^{(2)}, \ldots, x^{(2^m)}$
- If the received word is x_t, we compute $\delta(x^{(i)}, x_t)$ for $1 \leq i \leq 2^m$, and choose the first code word, say it is $x^{(s)}$, such that $\min_{1 \leq i \leq 2^m} \{\delta(x^{(i)}, x_t)\} = \delta(x^{(s)}, x_t)$
- That is, $x^{(s)}$ is a code word that is closest to x_t and the first in the list.
- If $x^{(s)} = e(b)$, we define the *maximum likelihood decoding function* d associated with e by $d(x_t) = b$.

How to correct errors?

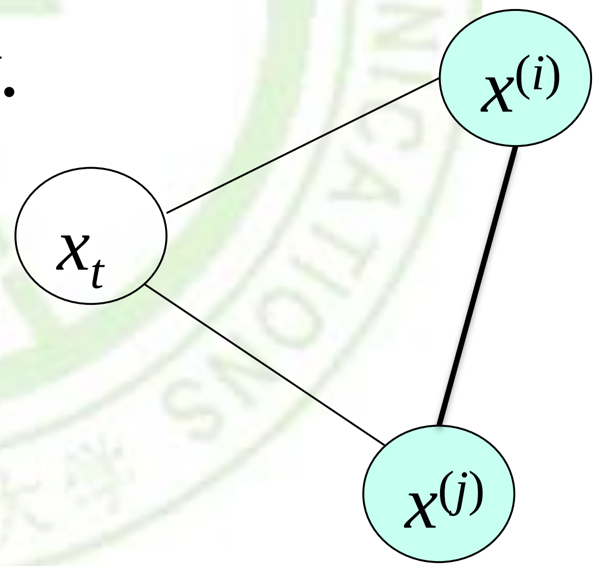
- If $\delta(x^{(i)},x_t) \le k$ and $\delta(x^{(i)},x_t) \le k$, where x would be transmitted with k or fewer errors.
- which one is x?

$\delta(x^{(i)}, x^{(j)}) > k$, *but may* $\le 2k$.

Since $\delta(x^{(i)}, x^{(j)})$

$$\le \delta(x^{(i)},x_t) + \delta(x^{(j)},x_t)$$

$$\le 2k$$



PROPERTIES OF DISTANCE FUNCTION

- Let x, y, and z be elements of B^n. Then
  - (d) $\delta(x, y) \le \delta(x, z) + \delta(z, y)$

- Proof of (d)
  - $|x \oplus y| \le |x| + |y|$; $\quad a \oplus a = \mathbf{0}$
  - $\delta(x, y) = |x \oplus y| = |x \oplus \mathbf{0} \oplus y|$

$$= |x \oplus z \oplus z \oplus y|$$

$$\le |x \oplus z| + |z \oplus y|$$

Theorem 1

- Suppose that e is an (m, n) encoding function and d is a maximum likelihood decoding function associated with e. Then
  - (e, d) can correct k or fewer errors
- if and only if
  - the minimum distance of e is at least $2k + 1$.

Correct k errors iff min{δ} ≥ 2k+1

Proof: 1. Assume $\min\{\delta(x^{(i)}, x^{(j)})\} \geq 2k+1$.

Let $x=e(b)$, x is transmintted with k or fewer errors, and x_t is received. $\delta(x,x_t) \leq k$.

If $\forall z \in e(B^m)$ *and* $z \neq x$, $\delta(x,z) \geq 2k+1$.

Since $\delta(x,z) \leq \delta(x,x_t)+\delta(x_t,z) \leq k + \delta(x_t,z)$.

Thus $\delta(x_t,z) \geq (2k+1)-k=k+1$.

$d(x_t)=b$. Hence (e,d) corrects k or fewer errors.

Correct k errors iff $\min\{\delta\} \geq 2k+1$

Proof: 2. Assume $\min\{\delta(x^{(i)}, x^{(j)})\}=r \leq 2k$ and $>k$. Let $x=e(b)$ *and* $x'=e(b')$ *with* $\delta(x, x')=r$,

x is transmintted with k or fewer errors, and x_t is received.

$\delta(x, x') \leq \delta(x,x_t)+\delta(x', x_t)$, Let $\delta(x',x_t) \leq \delta(x,x_t) \leq k$. and x' precedes x in list of code words;

$d(x_t)=x' \neq b$. *Then (e,d) has not corrected.*

How many errors can (e, d) correct?

- The (3, 8) encoding function $e: B^3 \to B^8$

$$\left.\begin{aligned}
e(000) &= 00000000 \\
e(001) &= 10011100 \\
e(010) &= 00101101 \\
e(011) &= 10010101 \\
e(100) &= 10100100 \\
e(101) &= 10001001 \\
e(110) &= 00011100 \\
e(111) &= 00110001
\end{aligned}\right\} \text{code word}$$

- and let d be an (8, 3) maximum likelihood decoding function associated with e.

How many errors can (e, d) correct?

- ***Solution:***
  - First compute the minimum distance of e, is 3.
  - By Theroem 1, $3 \geq 2k+1$, so $k \leq 1$.
  - Thus (e, d) can correct one error.

Constructing

maximum likelihood decoding function associated with a given group code

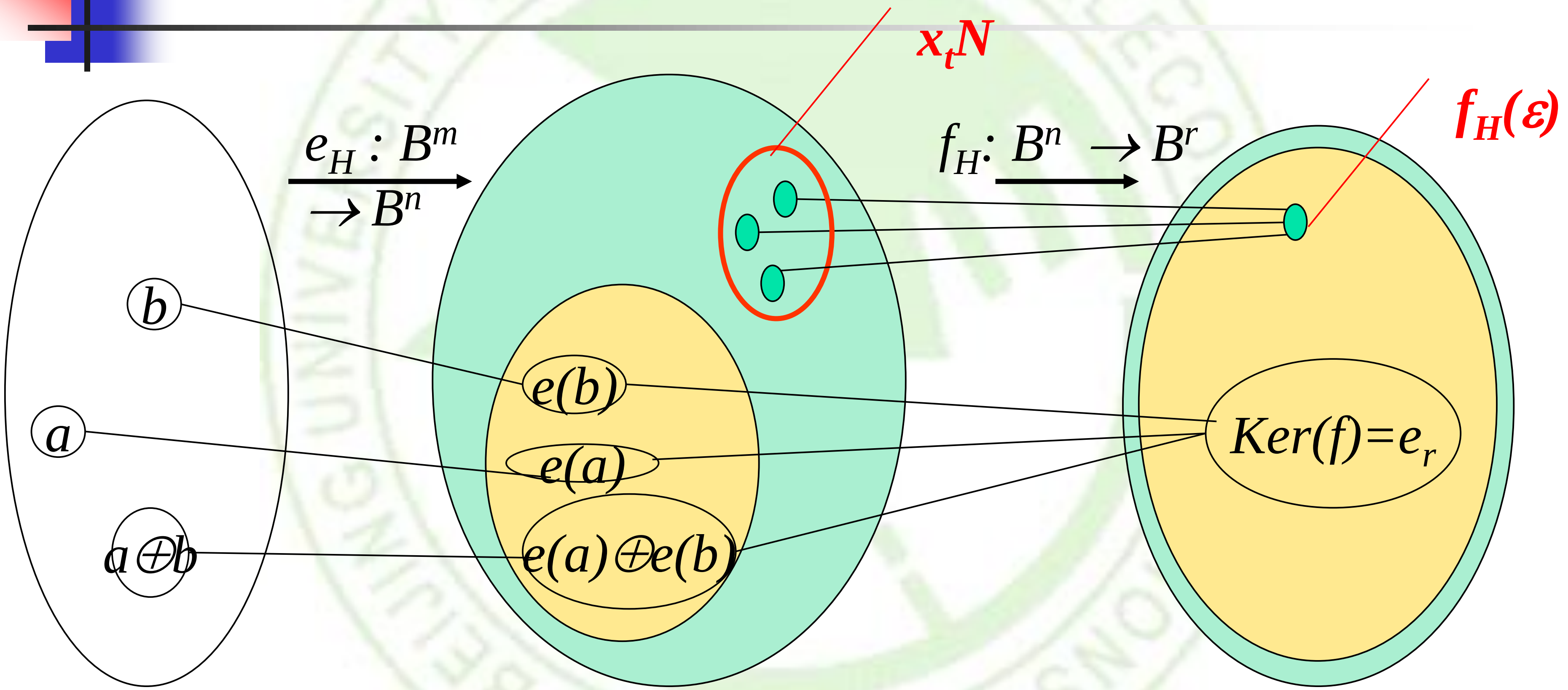
Zhang Yanmei

ymzhang@bupt.edu.cn

College of Computer Science & Technology

Beijing University of Posts & Telecommunications

(E,D) FUNCTION



e_H is a homomorphism and group code.

f_H is onto homomorphic, and $e(B^m)$ is ker(f).

Group code word

- Let $e: B^m \to B^n$ be an (m, n) encoding function that is a group code.
- Thus the set N of code words in B^n is a subgroup of B^n whose order is 2^m, say
  - $N = \{x^{(1)}, x^{(2)},\ldots, x^{(2^m)}\}$.

Theorem 2

- If K is a finite subgroup of a group G, then every left coset of K in G has exactly as many elements as K.

Coset leader – 陪集头

- Suppose that the code word $x = e(b)$ is transmitted and that the word x_t is received.
- The left coset of x_t is
  - $x_t \oplus N = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2m}\}$ where $\varepsilon_i = x_t \oplus x^{(i)}$
- if ε_j is a coset member with smallest weight, then $x^{(j)}$ must be a code word that is closest to x_t.
  - An element ε_j , having smallest weight, is called a *coset leader*. $\varepsilon_j = \min\{| x_t \oplus N | \} = x_t \oplus x^{(j)}$
  - $\boldsymbol{x_t \oplus \varepsilon_j} = x_t \oplus x_t \oplus x^{(j)} = \boldsymbol{x^{(j)}}$

Procedurec

- For obtaining a maximum likelihood decoding function d associated with a given group code e: $B^m \to B^n$
- ***Step 1***: Determine all the left cosets of $N = e(B^m)$ in B^n
- ***Step 2***: For each coset, **find a coset leader (a word of least weight)**.
- ***Step 3***: If the word x_t is received, determine the coset of N to which x_t belongs.
- ***Step 4***: Let ε be a coset leader for the coset determined in Step 3. Compute $x = x_t \oplus \varepsilon$. If $x = e(b)$, let $d(x_t) = b$.

Construct

- Determine all the left cosets of $N = e(B^m)$ in B^n
- ***N is a left coset.***
- *Find all distinct* $x_t N : x_t$ *is all case in* B^n .

  Since coset leader $\varepsilon \in x_t N$, *so* $[\varepsilon] = [x_t]$,

  thus $\varepsilon N = x_t N$.

  But ε *is a* **word of least weight**.

  We can list all ε, *and compute* εN.
- ***Note***: If $\varepsilon_i \in \varepsilon_j N$, *then* $[\varepsilon_i] = [\varepsilon_j]$, *then we must find* 2^r *not equalvalent coset leaders.*

Decoding table

- Constructing a decoding table, each row is a left coset of N with the first element $\varepsilon^{(i)}$ the coset leader.

$\vec{0}$	$x^{(2)}$	$x^{(3)}$	$\cdots$	$x^{(2^m-1)}$
$\epsilon^{(2)}$	$\epsilon^{(2)} \oplus x^{(2)}$	$\epsilon^{(2)} \oplus x^{(3)}$	$\cdots$	$\epsilon^{(2)} \oplus x^{(2^m-1)}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\epsilon^{(2^r)}$	$\epsilon^{(2^r)} \oplus x^{(2)}$	$\epsilon^{(2^r)} \oplus x^{(3)}$	$\cdots$	$\epsilon^{(2^r)} \oplus x^{(2^m-1)}$

- Find the location of word x_t in the table. The top element x of the column containing x_t, is the code word closest to x_t. $d(x_t) = substr(x) = b$.

Example 4

- Consider the (3, 6) group code
  - N = {000000, 001100, 010011, 011111, 100101, 101001, 110110, 111010}
  - $= \{x^{(1)}, x^{(2)}, \ldots, x^{(8)}\}$.

Example 4

Constructing decoding table:

000000	001100	010011	011111	100101	101001	110110	111010
000001	001101	010010	111110	100100	101000	110111	111011
000010	001110	010001	011101	100111	101011	110100	111000
000100	001000	010111	011011	100001	101101	110010	111110
010000	011100	000011	001111	110101	111001	100110	101010
100000	101100	110011	111111	000101	001001	010110	011010
000110	001010	010101	011001	100011	101111	110000	111100
010100	011000	000111	001011	110001	111101	100010	101110

001010	000110	011001	010101	101111	100011	111100	110000

Simplified decoding technique

- Suppose that the (m, n) group code is e_H: $B^m \to B^n$, where **H** is a given parity check matrix.

$$\mathrm{H} = \begin{bmatrix} \mathrm{H}_{m\times r} \\ \mathrm{I}_r \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1r} \\ h_{21} & h_{22} & \cdots & h_{2r} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mr} \\ \hline 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Theorem 3

- Then the function f_H: $B^n \to B^r$ defined by
  - $f_H(x) = x*\mathbf{H}, \; x \in B^n$
- is a homomorphism from the group B^n to the group B^r.
- If m, n, r, $\mathbf{H}$, and f_H are as defined, then
  - f_H is onto.

- $x_t N \leftrightarrow x_t{*}H$
- $\varepsilon_i N = x_t N \Rightarrow \varepsilon_i{*}H = x_t{*}H$

$$
\begin{tikzcd}
B^n \arrow[rr, "f_H"] \arrow[dr, "f_R"'] & & B^r \\
& B^n/ker(f) \arrow[ur, "\cong"'] &
\end{tikzcd}
$$

Syndrome – 校验子

- It follows from Corollary l of Section 9.5 that B^r and B^n/N are isomorphic, where
  - $N = \{x \in B^n \mid x*\mathbf{H} = \mathbf{0}\} = \ker(f_H) = e_H(B^m)$
- under the isomorphism g: $B^n/N \to B^r$ defined by
  - $g(xN) = f_H(x) = x*\mathbf{H}$
- The element $x*\mathbf{H}$ is called the *syndrome* of x

Theorem 4

- Let x and y be elements in B^n. Then
  - x and y lie in the same left coset of N in B^n
- if and only if
  - $f_H(x) = f_H(y)$
- if and only if
  - they have the same syndrome.

Proof

- It follows from Theorem 4 of Section 9.5
- that x and y lie in the same left coset of N in B^n
  - if and only if $(x^{-1}) \oplus y = x \oplus y \in N$.
- Since $N = \ker(f_H)$, $f_H(N) = 0_{Br}$
  - *iff* $f_H(x \oplus y) = 0_{Br}$
  - *iff* $f_H(x) \oplus f_H(y) = 0_{Br}$
  - *iff* $f_H(x) = f_H(y)$
  - *iff* $x*\mathbf{H} = y*\mathbf{H}$

- Q.E.D.

Decoding procedure

- Suppose that we compute the syndrome of each coset leader.
- If the word x_t is received, we also compute $f_H(x_t)$, the syndrome of x_t. By comparing $f_H(x_t)$ and the syndromes of the coset leaders, we find the coset in which x_t lies.
- Suppose that a coset leader of this coset is ε. We now compute $x = x_t \oplus \varepsilon$. If $x = e(b)$, we then decode x_t as b.

New procedure

- ***Step 1***: Determine all left cosets of $N = e_H(B^m)$ in B^n.
- ***Step 2***: For each coset, find a coset leader, and compute the syndrome of each leader
- ***Step 3***: If x_t is received, compute the syndrome of x_t and find the coset leader ε having the same syndrome. Then $x_t \oplus \varepsilon = x$ is a code word $e_H(b)$, and $d(x_t) = b$.

Example 5

- Consider the parity check matrix and the (3, 6) group code e_H: $B^3 \to B^6$.

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

$$\left.\begin{array}{l} e(000) = 000000 \\ e(001) = 001011 \\ e(010) = 010101 \\ e(011) = 011110 \\ \hline e(100) = 100110 \\ e(101) = 101101 \\ e(110) = 110011 \\ e(111) = 111000 \end{array}\right\} \text{code word}$$

Example 5

- N = {000000, 001011, 010101, 011110, 100110, 101101, 110011, 111000}

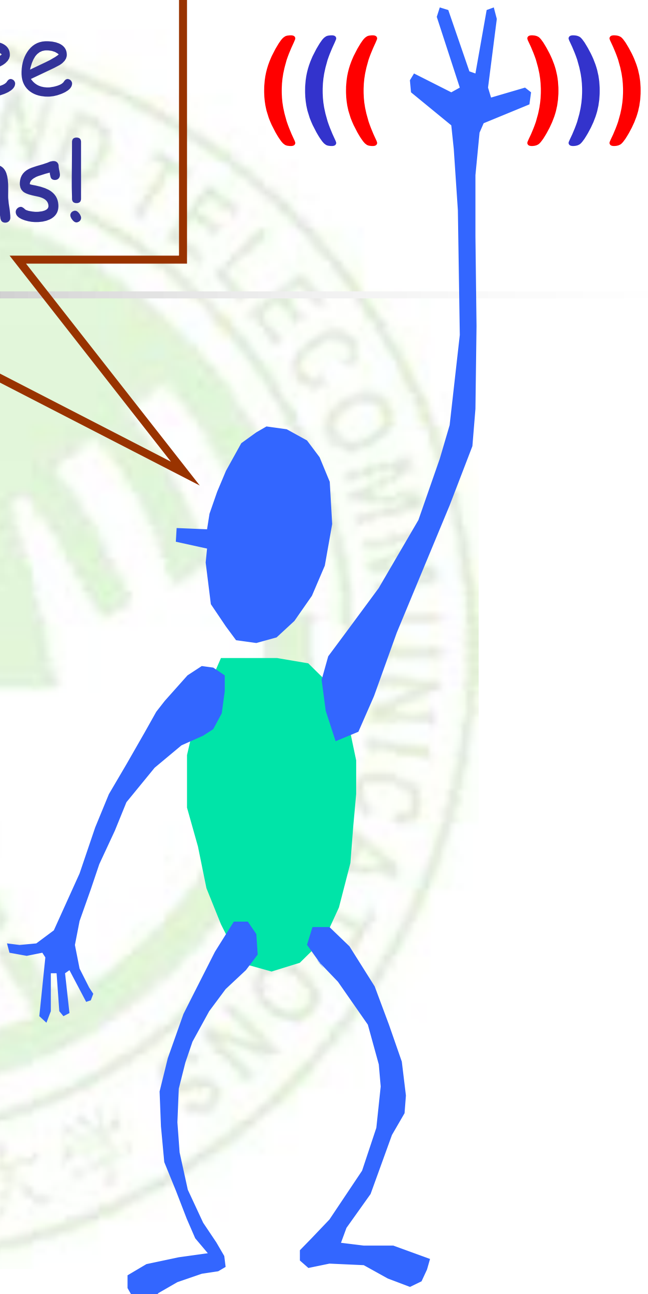
Syndrome of Coset Leader	Coset leader
000	000000
001	000001
010	000010
011	001000
100	000100
101	010000
110	100000
111	001100

Example 5

- If x_t = 001110, then $f_H(x_t) = x_t * \mathbf{H}$ = 101, same as ε=010000.
- $x = x_t \oplus \varepsilon$ = 001110 $\oplus$ 01000 = 011110 = e(011), so decode 001110 as 011.

Syndrome of Coset Leader	Coset leader
000	000000
001	000001
010	000010
011	001000
100	000100
101	010000
110	100000
111	001100

Please feel free to ask questions!



HOMEWORK

- 8,10,13,18,21,23 @421

编程作业：给定群码(m,n)编码函数e的H(读取文件,读取文件方式，第一行两个整数m,n，第二行$m\times(n-m)$个0或1，也就是矩阵H的上半部分，下半部单位矩阵自行生成)。

1. 计算与e相关的极大似然法能纠错的比特数
2. 交互方式给定的码字进行解码

Key ideas for review

- Message, word
- (m, n) encoding function, one-to-one
  - *Code word, parity check code*
  - *Detect, correct, k or fewer errors*
- Hamming distance
  - *Properties of distance*
- Group code and parity check matrix
  - *Minimum distance of a group code*
- Maximum likelihood technique
  - *Maximum likelihood decoding function*
  - *Syndrome and decoding procedure for group code*