Part I

Decoding and Error Correction

Definition (Decoding Function)

- Consider an (m, n) encoding function
  - $e : B^m \to B^n$
- 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.
- An onto function $d : B^n \to B^m$ is called an (n, m) decoding function associated with e if $d(x_t) = b' \in B^m$ is such that when the transmission channel has no noise, then $b' = b$, that is,
  - $d \circ e = 1_{B^m}$

Decoding Function

- The decoding function d 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 the decoding of improperly received words may or may not be correct.

Example (Parity Check Code)

- Define the decoding function $d : B^{m+1} \to B^n$.
  - If $y = y_1 y_2 \ldots y_m y_{m+l} \in B^{m+1}$, then $d(y) = y_1 y_2 \ldots y_m$
- Observe that if $b = b_1 b_2 \ldots b_m \in B^m$, then
  - $(d \circ e)(b) = d(e(b)) = b$
  - so $d \circ e = 1_{B^m}$
- For a concrete example, let $m = 4$
  - $d(10010) = 1001$
  - $d(11001) = 1100$

Example (Triple Encoding Function)

- Consider the $(m, 3m)$ encoding function. Define the decoding function $d : B^{3m} \to B^m$.
- Let $y = y_1 y_2 \dots y_m y_{m+1} \dots y_{2m} y_{2m+1} \dots y_{3m}$, then
  - $d(y) = z_1 z_2 \dots z_m$
  - where

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

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

Definition (Error Correction)

- 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.

Definition (Maximum Likelihood Decoding Function)

- 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
  - $d(x_t) = b$

Theorem (1)

- *Suppose*
  - e *is an* (m, n) *encoding function*
  - 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* $2k + 1$.

Example (How Many Errors Can (e, d) Correct?)

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

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

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

♪ Constructing maximum likelihood decoding function associated with a given group code

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.*

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

Definition (Coset Leader)

- 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 $x_t \oplus N = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2^m}\}$ 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.

A Maximum Likelihood Decoding Procedure

For obtaining a maximum likelihood decoding function d associated with a given group code $e : B^m \to B^n$

1. Determine all the left cosets of $N = e(B^m)$ in B^n
2. For each coset, find a coset leader (a word of least weight).
3. If the word x_t is received, determine the coset of N to which x_t belongs.
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 $d(x_t) = b$.

Decoding Table

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

$\overline{0}$	$x^{(2)}$	$x^{(3)}$	$\ldots$	$x^{(2^m-1)}$
$\varepsilon^{(2)}$	$\varepsilon^{(2)} \oplus x^{(2)}$	$\varepsilon^2 \oplus x^3$	$\ldots$	$\varepsilon^{(2)} \oplus x^{(2^m-1)}$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$
$\varepsilon^{(2^r)}$	$\varepsilon^{(2^r)} \oplus x^{(2)}$	$\varepsilon^{(2^r)} \oplus x^{(3)}$	$\ldots$	$\varepsilon^{(2^r)} \oplus x^{(2^m-1)}$

- If we receive the word x_t, we locate it in the table. If x is the element of N that is at the top of the column containing x_t, then x is the code word closest to x_t.
  - if $x = e(b)$, then $d(x_t) = b$.

Example (4)

- Consider the $(3,6)$ group code

$$\begin{aligned} N &= \{000000, 001100, 010011, 011111, 100101, 101001, \\ &\quad 110110, 111010\} \\ &= \{x^{(1)}, x^{(2)}, \ldots, x^{(8)}\} \end{aligned}$$

000000	001100	010011	011111	100101	101001	110110	111010
000001	001101	010010	011110	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

Example (4)

- Consider the $(3, 6)$ group code

$$\begin{aligned} N &= \{000000, 001100, 010011, 011111, 100101, 101001, \\ &\quad 110110, 111010\} \\ &= \{x^{(1)}, x^{(2)}, ..., x^{(8)}\} \end{aligned}$$

000000	001100	010011	011111	100101	101001	110110	111010
000001	001101	010010	011110	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

Example

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

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

Example

- 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.

Theorem (3)

- *If m, n, r, H, and f_H are as defined, then f_H is onto.*

Proof.

- Let $b = b_1 b_2 \ldots b_r$ be any element in B^r.
- Let $x = 0_1 \ldots 0_m b_1 b_2 \ldots b_r$
- Then $x * \mathbf{H} = b$.
- Thus $f_H(x) = b$, so f_H is onto.

❀

Definition (Syndrome)

- It follows from Corollary 1 of Section 9.5 that B^r and B^n/N are isomorphic, where
  - $N = \{x \in B^n | x * \mathbf{H} = 0\} = ker(f_H) = e_H(B^m)$
- under the isomorphism $g : B^n/N \to B^r$ defined by
  - $g(xN) = f_H(x) = x * \mathbf{H}$
- The element $x * H$ 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*

      $\Longleftrightarrow$
    - $f_H(x) = f_H(y)$

      $\Longleftrightarrow$
    - *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

    $\Longleftrightarrow$
  - $x \oplus y = (-x) \oplus y \in N$.
- Since N = ker(fH)
  - $x \oplus y \in N$

    $\Longleftrightarrow$
  - $f_H(x \oplus y) = 0_{B^r}$
  - $f_H(x) \oplus f_H(y) = 0_{B^r}$
  - $f_H(x) = f_H(y)$

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

1. Determine all left cosets of $N = e_H(B^m)$ in B^n
2. For each coset, find a coset leader, and compute the syndrome of each leader
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 $e_H : B^3 \to B^6$.

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \left.\begin{aligned} e(000) &= 000000 \\ e(001) &= 001011 \\ e(010) &= 010101 \\ e(011) &= 011110 \\ e(100) &= 100110 \\ e(101) &= 101101 \\ e(110) &= 110011 \\ e(111) &= 111000 \end{aligned}\right\} \text{code word}$$

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
110	001100

Example (5)

- If $x_t = 001110$, then $f_H(x_t) = x_t * \mathbf{H} = 101$, same as $\varepsilon = 010000$.
- $x = x_t \oplus \varepsilon = 001110 \oplus 010000 = 011110 = e(011)$, 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
110	001100

Homework

- $8, 10, 13, 18, 21, 23@page421$
- 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