Lecture #1

I. Motivation and Overview

A. Starting from Basics

1. Simple Examples

a. Odd or Even Parity

used to set our moderns
parity: "odd" or "even"

Suppose "even" parity, bit set so you get an
even number of 1's

Data: 10110100

get at receiver:

10100100 - odd words!
must be an error - detected

know it should be even - but there are lots
of errors that are "close"
cannot correct it!

get at receiver:

10111000 - even... fine

cannot detect two errors

single-error detecting, no error correcting code SED
What is happening geometrically?

Let's consider the following:

- $p = 0.1 \implies p(E) = 0.008$
- $p\text{ (correct)} = (1-p)^3 + 3p(1-p)^2$
- $p = 0.1 \implies p(\text{correct}) = 0.008$

So, $\hat{p} = \text{some estimate}$ is correct if $\hat{p} - p > 3\sqrt{\frac{p(1-p)}{n}}$. Suppose $\hat{p} - p = 0.10$. Then $0.008 \leq 0.10$

And, we have $\text{send 000}$

But, we want to correct errors. How?

- Talk about the obvious things.
Two choices:

1. Feel stuff or just move slower.
2. Send stuff as slow as possible.

Thus after you start you get up to the actual, phlegm.

\[ T = \frac{A}{\text{steps} / \text{iii}} \]

Prove:

\[ \frac{5}{2} + \frac{1}{2} = \frac{3}{2} \]

(5) \[ \frac{5}{2} \]

(2) \[ \frac{1}{2} \]

(3) \[ \frac{3}{2} \]
Lecture #2

I Motivation and Overview
A Starting from Basics
1 Simple Examples

a Odd or Even Parity

Suppose "even"

\[
p_{\text{even}} = \frac{10110101}{0101}
\]

SEED

b \((L, 1)\) repetition codes \((L \text{ odd})\)

\[
P(F) = \sum_{m=\frac{L+1}{2}}^{L} \binom{L}{m} p^m (1-p)^{L-m} \downarrow \text{ as } L \uparrow
\]

but rate loss is problematic \((n,k)\) code

Key tradeoff: rate vs. error correction

generically

\((5,1)\)

\[
\begin{array}{cccccc}
0000 & 0111 & & & & \\
X < & d=5 & & & & X
\end{array}
\]

How about a \((5,2)\) code? Need \(n\) codewords

\[
10110
\]

will be closer together.
2 Channel Coding Theorem
(Shannon, 1948)

Theorem: For any communication channel, there exists a number \( C \) such that for any rate \( R < C \), the probability of error \( P(e) \) converges to zero as \( n \to \infty \).

Proof:
1. Take a block of binary bits:

\[
\begin{array}{c}
\vdots \\
0 \ 0 \ 0 \ \ldots \ 0 \\
0 \ 0 \ 0 \ \ldots \ 01 \\
0 \ 0 \ 0 \ \ldots \ 10 \\
\vdots \\
0 \ 0 \ 0 \ \ldots \ 11
\end{array}
\]

2. Show the average of all codes does well enough.

\[ \Rightarrow \text{there must be a good code} \]

Problems:

- Continuity of good code not given
- Long unstructured code — very hard

Have spent the last 60 years trying to achieve this — and now we are finally coming pretty close.
Now it's rate vs. error correcting capability as "reasonable" decoding complexity.

Define a code $C$ is **linear** if $x \in C, y \in C \Rightarrow x + y \in C$.

Define a cyclic code is a linear code such that each cyclic shift of $x_1$ codeword in $C$ also...
Towards Realizable Good (non-repetition) Codes

(7,4) Hamming code [Hamming, 1954]

Cute idea:

3 links: A, B, C

7 bit locations

Encoder: Put your 4 bits in spots 1, 2, 3, 4
Complete 5, 6, 7 so that each circle (A, B, C) has even parity

Decoder
The "parity check" for this code is to add all locations "mod 2" and make sure it is zero.

Need a better idea? (Hamming, 1949)

1. A
   - 1
   - 5
   - 11
   - 7
   - 0
   - 2
   - 1
   - 3

Red error violates parity check B and C. Flip bit that is common to those circles.

2. Put information bits in 1, 2, 3, 4. Complete 5, 6, 7 so each circle has even parity. Code corrects one error.

3. Make table: each row is a parity check containing is for bits that parity check adds.

<table>
<thead>
<tr>
<th>A</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Hamming code
Def: \((n-k) \times n\) 

This is the parity check matrix \(H\).

- Number of info bits: \(k\)
- Number of parity checks: \(n-k\)
- Code length: \(n\)

Note: \(H_y = 0\) (mod 2 addition) 

(i.e. \(e\) is a subspace)

Suppose we receive \(y\) and want to calculate which parity checks are violated.

\[
\delta = H_y^T \quad \text{(all additions mod } 2)\]

Proof: The syndrome \(\delta\) of length \(n-k\) has a 1 wherever a parity check is violated.

We want every error pattern that we wish to correct to have a distinct syndrome.

Suppose a codeword \(c\) is transmitted and \(e\) is the error vector. Then \(y = c + e\) (mod 2 addition)

\[
\delta = H_y^T = H (c^T \oplus e^T) = H c^T \oplus H e^T = H e^T
\]
Note that any single error gives a column of $H$.

The Decoding Algorithm for a SEC (single-error correcting code)

1. Find $z$
2. Find column of $H$ that matches $z$'s correct bit corresponding to that column.

Example

$e = 1000101$
$e = 0010000$
$y = 1010101$

$Hy^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ = column three of $H$

$\Rightarrow$ Fix third bit

$\hat{e} = 1000101$

(b) Generator Matrix

Define: A code $e \in \{0, 1\}^{n-k+1}$ is linear if $e_1 \oplus e_2 \in e, \forall e_1, e_2$. 
I. Motivation and Overview
   A. Starting from Basics

   Rate vs. Error correction or "reasonable" complexity

II. Towards Realizable Codes

   1. Hamming Codes

   \[
   \begin{bmatrix}
   1 & 1 & 0 & 1 & 1 & 0 & 0 \\
   1 & 0 & 1 & 1 & 0 & 0 & 1 \\
   0 & 1 & 1 & 0 & 1 & 0 & 0
   \end{bmatrix}
   \]

   \[s = H(e^T + e'^T) = H e^T\]

   SEC because all single errors map into different \(s\).

   \[H e^T = 0 \iff \text{parity check value} \]
2. A Simple Convolutional Code

Consider the following very simple encoder

```
Consider the following very simple encoder tree.

+------------------+
|                  |
| info             |
|                  |
+------------------+
```

```
+------------------+
|                  |
| code bit 1       |
|                  |
+------------------+
```

```
+------------------+
|                  |
| code bit 2       |
|                  |
+------------------+
```

Can show dmin = 5 for a simple R = 5 code! 😊

And works great when receiving not just 0's and 1's 😊

...but hard to analyze! 😱

Block codes are for textbooks, convolutional codes are for real systems. 😊
Applications of Error Control Coding
Costello et al.

Deep space (A/JoJ)

\[ \text{dB} = 1,000,000 \times (140^{-0.5} \text{ dB}) \]

(32,4) \( n - m \) \( d_{\text{min}} = 16 \)
\[ r = \frac{7}{4} \]

Voyager 1,2, 1977 \( (3,1,7) \) \( \text{unc.} \)

(2,1,7) \( \text{over} \) \( (253,322) \) \( \text{A-3} \)

(4,1,5) \( \text{unc.} \)

Turbo

2 \( T(n - m) \)

3 \( \text{del. stat.} \)

blue

4 \( \text{CC-ComA} \)
II  Introduction to Channel Coding Practice

A  Generator Matrices

1  Generator Matrix

Recall that an \((n,k)\) code \(C\) is linear if for all \(c_1, c_2 \in C\),
\[c_1, c_2 \in C.\]

[Note: Parity check codes are linear]

\[H e_1^T = 0 \quad \text{and} \quad H e_2^T = 0\]

\[\Rightarrow H (e_1^T \otimes e_2^T) = 0\]

\[\Rightarrow e_1 \otimes e_2 \in C\]

Also, note that \(e_1 \otimes e_2 \in C\) for \(c_1 = (0,1)^T\)

\[\Rightarrow e_2 \in C\]

\[\Rightarrow \text{codewords form a k-dimensional subspace of} \ \mathbb{F}_2^n\]

\[\Rightarrow \text{code is the row space of a matrix with} \ k \ \text{linearly independent codewords as rows}\]
Fact: Parity check codes are linear.

\[ H e_1^T = 0 \quad \text{and} \quad H e_2^T = 0 \quad \Rightarrow \quad H(e_1^T + e_2^T) = 0 \]

\[ \Rightarrow e_1 + e_2 + e \]

Also, \( e\in\mathbb{R}^n \) for \( e\in\mathbb{R}^n \).

\[ \Rightarrow \quad \text{codewords form a k-dimensional subspace of the vector space } \mathbb{R}^n. \]

\[ \Rightarrow \quad \text{The code is the rowspace of a matrix} \]

\[ G = \begin{pmatrix} g_1^T \\ g_2^T \\ g_3^T \end{pmatrix} \]

\[ x \in C \iff x = uG \]

\[ x \in C \iff Hx^T = 0 \]

\[ \Rightarrow \quad O = Hx^T = H(uC)^T = HG^T u \quad (0 \in C) \]

\[ \Rightarrow \quad HG^T = 0 \]

\[ \Rightarrow \quad \text{If } C = (I_n | A) \]

\[ H = (A^T | I_{n-k}) \]
2 Error Correction Capabilities

a. Some Definitions

**Definition:** The *Hamming distance* \( d_H(x, y) \) is the number of places in which \( x \) and \( y \) differ.

**Definition:** The *minimum distance* \( d_{H, \text{min}}(C) \) is

\[
\min_{e, e' \in C, e \neq e'} d_H(e, e')
\]

**Definition:** The *Hamming weight* of \( x \):

\[ \text{wt}(x) = d_H(\mathbf{0}, x) \]

4. **Linear Codes**

**Theorem:** For a linear code \( C \).

\[
\min_{e, e' \in C, e \neq e'} d_H(e, e') = \min_{e \in C} \text{wt}(e)
\]

**Theorem:** A linear code \( C \) can correct

\[
t = \left\lfloor \frac{\text{wt}_{\text{min}}(C) - 1}{2} \right\rfloor
\]

**Errors**

\[
\left\lfloor \frac{\text{wt}_{\text{min}}(C) - 1}{2} \right\rfloor
\]
II Introduction to Channel Coding Practice

A The Basics

A \( \frac{1}{C} \) (n, k) code

\[ \begin{array}{c}
  \frac{1}{C} \\
  \begin{array}{c}
    b_0, \ldots, b_{n-k} \\
    00 \ldots 0 \\
    00 \ldots 1
  \end{array}
\end{array} \]

need

Recall a linear code is closed under addition and scalar multiplication:

\[ \sum_{i=1}^{m} g_i, \ldots, g_i \in \mathbb{F}_2 \]

\[ \sum_{i=1}^{m} 2^m \beta = \mu G \]

for some \( \mu \)

shown

\[ AG^T = 0 \]

\[ C = (I_k | A) \]

\[ H = (A^T | I_{n-k}) \]

2 Error Corrective

\[ \begin{array}{c}
  d_{\min} \\
  d_{\min}(\mathbf{e}) \\
  d_{\min}(\mathbf{e}_1, \mathbf{e}_2)
\end{array} \]

\[ \min_{\mathbf{e}_1, \mathbf{e}_2} d_{\min}(\mathbf{e}_1, \mathbf{e}_2) = \min_{\mathbf{e}_1, \mathbf{e}_2} \omega(d_{\min}(\mathbf{e}_1, \mathbf{e}_2)) \]

\[ H \mathbf{e} = 0 \]
Def: The Hamming weight of \( x \) is
\[ w(x) = \text{Ham}(0, x) \]

For a linear code,
\[ \min_{0 \leq e_i, e_j \leq \epsilon_i, \epsilon_j} \text{Ham}(e_i, e_j) = \min_{0 \leq e_i} \text{Ham}(0, e_i) = \min_{0 \leq e_i} \text{wt}(e_i) \]

**Fact:** A code is \( t \)-um correct if
\[ t = \left\lfloor \frac{\text{Ham}(0, e) - 1}{2} \right\rfloor \] errors

Thus, the minimum distance is critical. How do I find it from \( H \)?

\[ H y^T = 0 \iff y \in \mathbb{F}_2^* \]

\[ d_0 y_0 + d_1 y_1 + \ldots + d_{n-1} y_{n-1} = 0 \iff y \in \mathbb{F}_2^* \]

\[ \text{Minimum weight of code is smallest number of columns of } H \text{ that sum to yield zero.} \]
Lecture 23

Bounds on \( d_m \) (or on the error correcting \( t \))

(Any block codes.)

Hanning Bound

An \((n, k)\) block that is \( t \)-error correcting satisfies

\[
\sum_{t=0}^{t} \binom{n}{m} \leq 2^{n(1-r)}
\]

Proof

Suppose there are \( m \) codewords. Each codeword \( \xi_i \) and the sets of vectors \( \xi_i \), \( d_H(\xi_i, \xi_j) \) must not overlap any other sphere. Thus,

\[
m \sum_{t=0}^{t} \binom{n}{m} \leq 2^n
\]

\[
\sum_{t=0}^{t} \binom{n}{m} \leq 2^{n-k} = 2^{n(1-r)}
\]

If \( m = \frac{2^n}{\sum_{t=0}^{t} \binom{n}{m}} \), the code is perfect.

Gilbert-Varshamov Bound

An \((n, k)\) block code with minimum distance \( d_{\text{min}} \) can be found if

\[
\sum_{t=2}^{t} \binom{n}{m} \leq 2^{n(1-r)}
\]
Proof:

Put all $2^n$ sequences in a jar. Draw one out and remove all sequences within chain $\mathcal{C}$ of it:

$$\sum_{1=0}^{d_{m-1}} \binom{n}{2}$$

Now reach into the jar and repeat until we are out of sequences. This can continue as long as

$$\sum_{1=0}^{d_{m-1}} \binom{n}{2} \leq 2^n$$

$$\sum_{1=0}^{d_{m-1}} \binom{n-1}{2} \leq 2^{n-1}$$

This code has distance $\delta_n$ at least by construction.
Standard Array Decoding

Given a received $v$, we form $s = Hy^T$ and want to find $e \in E$.

$$s = He^T \quad (*)$$

Suppose $e_1$ is one solution $\iff e_1 + e$ is a solution for $e \in E$.

$\implies$ There are $2^k$ solutions for each $s$.

Noting that there are $2^{n-k}$ syndromes and that a vector $y$ cannot be the solution to $(*)$ for two distinct syndromes, the possible received vectors ($2^n$ of them) can be divided into sets of size $2^{n-k}$, one set for each syndrome, called cosets of $E$.

Form standard array:

<table>
<thead>
<tr>
<th>$s$</th>
<th>coset</th>
</tr>
</thead>
<tbody>
<tr>
<td>00...00</td>
<td>$e$</td>
</tr>
<tr>
<td>00...01</td>
<td>$e + x_1$</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td>11...11</td>
<td>$e + x_2^{n-k}$</td>
</tr>
</tbody>
</table>
Lecture #5

II. Intro to Channel Coding Practice
   A. Basics

   1. Generator

   2. Error Correction

      c. Bounds on code

      Hamming: If a code exists,

      \[ \sum_{k=0}^{t} \binom{n}{k} \leq 2^{n(1-r)} \]

      \[ \sum_{k=0}^{d_{min}-1} \binom{n}{k} \leq 2^{n(1-r)} \] (positive)

      \[ \sum_{k=0}^{d_{min}} \binom{n}{k} \leq 2^{n(1-r)} \] (negative)

      (Gries' Varshamov)

      A code exists if

      \[ \sum_{k=0}^{d_{min}-1} \binom{n}{k} \leq 2^{n(1-r)} \] (positive)

   3. Standard Array Decoding

      Form standard array

      \[ \Sigma = H \Sigma^T = H (\Sigma \oplus e)^T \]

      \[ \Sigma = H \Sigma^T = H (\Sigma \oplus e)^T \]

      Adding victim

      Null space also gives a solution.
To decide:

Off-line, find vector of lowest weight in each coset, called coset leaders.

1. Form $\mathbf{z} = H\mathbf{y}^T$
2. Find coset leader $\mathbf{e}$ for coset of $\mathbf{z}$
3. Output $\mathbf{z} = \mathbf{y} + \mathbf{e}$

Example $(5,2)$ SEC code

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

$\mathbf{z}$

<table>
<thead>
<tr>
<th></th>
<th>$\mathbf{e}$</th>
<th>00000</th>
<th>10101</th>
<th>01011</th>
<th>11110</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>00001 + $\mathbf{e}$</td>
<td>00001</td>
<td>10100</td>
<td>01010</td>
<td>11111</td>
</tr>
<tr>
<td>010</td>
<td>00010 + $\mathbf{e}$</td>
<td>00010</td>
<td>00111</td>
<td>01001</td>
<td>11100</td>
</tr>
</tbody>
</table>
Determine the covering radius of a code is the maximum distance of a received vector from a codeword.

Recall, for linear codes,

\[ d_{\text{min}}(C) = \min_{x, y \in C} d_h(x, y) = \min_{0 \neq z} w_2(z) \]

How do I figure this out by looking at \( H \)?

- **Maximum number of columns of \( H \) that sum to 1**

- **Shortening a code**

  Suppose I have an \((n, k)\) code and I remove a column of \( H \). What happens?

  \((n-1, k-1)\) code. What happens to \( \min \)?

  The same, but have lost rate. Okay... applications don't care.

- **Extending a code**

  Suppose I have an \((n, k)\) code of odd \( n \).

  Add one more row to get \((n, k-1)\) code with \( d + 1 \)!
Defn: (Hamming) distance between two words is the number of places in which they differ.

Defn: The minimum distance of the code is the minimum distance between a pair of codewords.

If code is linear, \( d(x_1, x_2) = d \), then, since \( x_2 + x_1 \in C \), \( d (0, x_2 - x_1) = d \).

- \( 0 \) always belongs to a linear code.

Defn: Hamming weight of a word is the number of non-zero elements in the word.

- For a linear code, minimum distance is the minimum non-zero weight.

If two words are distance \( d \) apart and one is transmitted, then if \( w(c) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \), the new word is closer to the transmitted than other.

For a code with minimum distance \( d \), can correct \( \frac{d-1}{2} \) errors.

The weight enumerator of the code is a polynomial

\[
A(x) = 1 + A_1x + \ldots + A_{d-1}x^{d-1} + A_dx^d
\]

where \( A_j \) = \# of codewords of weight \( j \).

\[ \text{e.g. } (7, 4) \text{ Hamming: know we have all } 7 \text{ s and all } 0 \text{'s. Since all } 1 \text{s in } x, \text{ and } \bar{x}, \text{ complement}
\]

must appear together and \( W(x) = 7 - w(x) \)
We consider a code of words

when we use as error detection only
(i.e., reject if error detected - parity
checks not satisfied)

Then Pr undetected error is

\[
\Pr \text{undetected error} = \sum_{\mathbf{w} \in S} A_2 \cdot p^2 (1-p)^{n-2} \\
= (1-p)^n \sum_{\mathbf{w} \in S} A_2 \cdot \left( \frac{p}{1-p} \right)^2 \\
= (1-p)^n \left[ A(x) - 1 \right] \sum_{\mathbf{w} \in S} \frac{p^2}{1-p}
\]

In general, let C be used in a
binary input d.m. channel, output alphabet \( Y \)
we use a maximum likelihood decoding rule.
Then \( \Pr = A(x) - 1 \) where

\[ Y = \sum_{\text{y}} \sqrt{pla(y,0)pla(y,1)} \]  
(Bhattacharyya Bound)

c.e. BSC \[ \gamma = 2 \sqrt{2(1-c)} \]

Proof

Let \( \mathbf{C} = \mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{n-1} \)

\( \mathbf{c}_0 = (000 \ldots 0) \) - assume this transmitted.

and let \( \Pr^{(n)} = \text{prob. of error given codeword transmitted} \)

\[ \Pr^{(n)} = ? \) - we make an error if \( pla(y,2) > pla(y,0) \)
and maybe if \( pla(y,0) = pla(y,2) \)

\( \Pr \) is pessimistic: This wrong \( \Rightarrow \) error \( \Rightarrow pla(y,2) > pla(y,0) \)

\( \text{Moreover, if } \Pr^{(n)} = \text{error} \Rightarrow pla(y,2) > pla(y,0) \)
then \( P_E^{(x)} \leq \sum_{i=1}^{n-1} Q_i \), where \( Q_i = \sum_{y \in Y_i} P(y) \).

Since \( \sqrt{\frac{1}{\sum_{y \in Y_i} P(y)}} = 1 \) for \( y \in Y_i \):

\[
Q_i \leq \sum_{y \in Y_i} \sqrt{P(y)} \cdot P(y) = \sum_{y \in Y_i} \sqrt{P(y)} P(y)
\]

Now, \( P(y) = \prod_{i=1}^{n} P(y_i) \).

\[
\therefore Q_i \leq \prod_{i=1}^{n} \sum_{y \in Y_i} \sqrt{P(y)} P(y) = \prod_{i=1}^{n} \sqrt{P(y_i)} P(y_i)
\]

Inner sum is 1 if \( x_{i,k} = y_{i,k} \)

\( x_{i,k} \neq y_{i,k} \)

\[\Rightarrow Q_i \leq A_{\mathcal{H}}(x_0, \varnothing, \emptyset, \emptyset)\]

\[\therefore P_E^{(x)} \leq \sum_{i=1}^{n-1} A_i^{(x)} \quad A_i^{(x)} = \# \text{ of codewords distance } i \text{ from } 0.
\]

\[= \sum_{i=1}^{n-1} A_i^{(x)} \quad A_i = A_i
\]

\[= A(\mathcal{X}) - 1 \quad \text{(note: same for other codewords also)}
\]

e.g. \( C = \{00000, 11111\} \) over a BSC

\[P_E \leq 32 \left[ \varepsilon (1 - \varepsilon) \right]^{5/2}
\]

\[P_E \geq 10 \varepsilon^3 (1 - \varepsilon)^2 + 5 \varepsilon^4 (1 - \varepsilon) + \varepsilon^5 = 10 \varepsilon^3 - 15 \varepsilon^4 + 6 \varepsilon^5
\]

So, for small \( \varepsilon \), it's \( 32 \varepsilon^{3.5} \) vs. \( 10 \varepsilon^3 \)-a reasonable bound.
 Lecture 

ECE 6471

II Intro to Channel Coding Practice

A Basics

$C, H$

4. $H$ and $d_{\min}$

For a linear code

$$d_{H,\min}(e) = \min_{i \neq j} d_H(e_i, e_j) = \min_{i \neq j} wt(e_i)$$

$\min$ # of columns of $H$ is $E$

$wt. i$: avoid $0$'s column

$wt. 2$: avoid identical cols.

$wt. 3$: All columns distinct - good.

Shortening a code

From above, if I remove columns, $d_{H,\min}(e)$ cannot go down.

Thus, and $(n, k, t)$ code can be changed to

$(n-m, k-m, t)$ for any $m(e_k)$ by removing

cols of $H$
extending a code

Suppose I have a \((n, k)\) code of odd \(d_{\text{min}}\).

Add 1 row to \(H\).

\[ r = \frac{k-1}{n} \quad \text{code of } d_{\text{min}} + 1 \]

Rate goes down (of course) by only keeping codewords of even parity.

Any other way to give all codewords even parity?

Add new parity bit to end to force even parity.

\[ r = \frac{k}{n+1} \quad \text{code of } d_{\text{min}} + 1 \]

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

B Weight Enumerators

1. Definitions

Definition The weight enumerator of the code is the polynomial

\[ A(x) = 1 + A_1 x + A_2 x^2 + \ldots + A_n x^n \]

where \( A_i \) = \# of codewords with weight \( i \).
Example

What is the weight enumerator of the (7,4) Hamming code?

Recall $d_{\min} = 3 \Rightarrow A_0 = 1$
$A_1 = 0$
$A_2 = 0$
$A_3 > 0$

**Trick:** Is all 1's in code? Check $H$. Yes!

$\Rightarrow A_7 = 1$
$A_6 = 0$
$A_5 = 0 \land d_{\min} = 3$
$A_4 ?$

How do the 1U remaining break among $A_3, A_4$?

**Evenly, because all 1's is there.**

2 Error Probabilities and Weight Enumerators

a Error Detection

Suppose all we want to do is ask did an error occur on the channel? (i.e. $\text{wt}(e) \neq 1$)
(No error correction)

$\hat{s} = He^T$

If $\hat{s} \neq 0$, we know an error occurred.

$\hat{s} = 0$, we don't really know... it's equal to a rock word
\[ P(\text{undetected error}) = P(e = c_2^n) U e = c_2^n \cup \cdots \cup \{e = c_{2^k, 1}\} \]
\[ \leq \sum_{i=1}^{2^k - 1} P(e = c_i) \]
\[ \leq \sum_{i=1}^{2^k - 1} P(A_i) \leq \sum_{i=1}^{2^k - 1} P(A_i) \]
\[ = \sum_{i=1}^{2^k - 1} n^{\omega(t(c_i))} (1 - \rho)t(c_i) \]
\[ = (1 - \rho)^n \sum_{i=1}^{2^k - 1} (\rho / (1 - \rho))^{\omega(t(c_i))} \]
\[ = (1 - \rho)^n \sum_{i=1}^{2^k - 1} A_i (\rho / (1 - \rho))^i \]
\[ = (1 - \rho)^n [A(x) - 1] \quad \text{where } x = \rho / (1 - \rho) \]

Theorem 1:
Now, let's look at error probability.

Consider a code \( E = \{ e_0, e_1, \ldots, e_{2^k - 1} \} \)

Let \( P_E^{(1)} \) = prob of error given \( x \) transmitted

First, consider \( P_E^{(1)} \).

Make an error if
\[ d_H(x, e_i) \leq d_H(x, e_0) \]

For some \( i \neq 0 \)
$$P_{E}^{(a)} = \mathbb{P} \left( \cup \{ d_{H}(y, \varepsilon_{a}) \leq D_{H}(y, \varepsilon_{a}) \} \right)$$

$$\Rightarrow \sum_{j=1}^{2^{k-1}} P \left( \{ d_{H}(y, \varepsilon_{a}) = d_{H}(y, \varepsilon_{a}) \} \right)$$

$$\leq \sum_{j=1}^{2^{k-1}} \int_{y} P \left( \frac{y-y_{a}}{x_{a}} \right) d_{H}(y, \varepsilon_{a})$$

$$= \sum_{j=1}^{2^{k-1}} \int_{y} P \left( \frac{y-y_{a}}{x_{a}} \right) \sqrt{p(y|x_{a})} \sqrt{p(y|x_{a})} d_{H}(y, \varepsilon_{a})$$

$$= \sum_{j=1}^{2^{k-1}} \int_{y} \sqrt{p(y|x_{a})} \sqrt{p(y|x_{a})} d_{H}(y, \varepsilon_{a})$$

$$= \sum_{j=1}^{2^{k-1}} \int_{y} \prod_{k=1}^{n} \left[ \frac{p(y_{k}|x_{a,k}) p(y_{k}|x_{a,k})}{p(y_{k}|x_{a,k}) p(y_{k}|x_{a,k})} \right] d_{H}(y, \varepsilon_{a})$$

$$= \sum_{j=1}^{2^{k-1}} \int_{y} \prod_{k=1}^{n} \left[ \frac{1}{2} \right] \left( D \left[ \sqrt{p(y_{k}|x_{a,k}) p(y_{k}|x_{a,k})} \right] \right) d_{H}(y, \varepsilon_{a})$$

$$= \sum_{j=1}^{2^{k-1}} \int_{y} D_{H}(y, \varepsilon_{a}) = D_{H}(x_{a}, \varepsilon_{a})$$

$$= A(0) = 1$$

(\text{note:} \quad P_{E}^{(a)} \text{ is independent for } a \quad \text{linear code})

\text{linear code = geometrically uniform)
Example

For Bsc

\[
D = \sqrt{\int_{Y} p(y) [p(y) 11] dy} = \sqrt{p(1-p)} + \sqrt{p(1-p)} = 2 \sqrt{p(1-p)}
\]

Suppose \( E = [0000 1111111] \)

\[
P_E \leq 32 [p(1-p)]^{316}
\]

\[
P_E = 10 p^3 (1-p)^2 + 5 p^4 (1-p) + p^5
\]

\[
= 10 p^5 - 15 p^4 + 6 p^5
\]
3 Weight Enumerators of Cosets

Define consider a code \( \mathcal{C} \) with generator \( G \) and parity check \( H \). The dual code \( \mathcal{C}^\perp \) is the code with generator \( H \) and parity check \( G \).

1. Every code has a unique dual
2. \( (\mathcal{C}^\perp)^\perp = \mathcal{C} \)
3. \( \mathcal{C}^\perp \) consists of all words \( \mathbf{w} \) s.t. \( \mathbf{w}^T \cdot \mathbf{e}_i = 0 \), \( \forall \mathbf{e}_i \in \mathcal{E} \)

\[ (7,4) \]

Dual of Hamming code is called the \( \text{Simplex} \) code.

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

\( \mathcal{E}^\perp = \{ \mathbf{e}_0, r_1, r_2, r_3, r_4, r_2r_3, r_2r_4, r_3r_4 \} \)

\[ A_{\mathcal{C}^\perp}(x) = 1 + 7x^4 \]

\( 2^4 \) syndromes. (and thus \( 16 \) cosets)

Can you find the weight enumerators of the cosets?
$(7, 3, 4)$ - dual of Hamming code
need coset weight enumerators

weight enumerator is $1 + 7x^3$

1. Since all codewords have even weight, then either every word in a coset has even wt. or "odd wt." odd wt.

(Because $wt(w+c) = wt(w) + wt(c) - 2 \cdot wt(w \cap c) = parity of w$)

2. We need to show covering radius is less than 4 (c.e. $\leq$ maximum wt. of any coset leader or joint leader = max. distance from any word to nearest codeword)

Proof: Suppose not - try all of all codewords:

<table>
<thead>
<tr>
<th>$w$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$w_2$</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$w_3$</td>
<td></td>
<td></td>
<td>8</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$w_4$</td>
<td></td>
<td></td>
<td>6</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$w_5$</td>
<td></td>
<td></td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...not possible min. dist violations
Eliminating case c(i): (c(ii) & (iii)) similar

take one of wt. 4: \( \text{IIII} \text{I}000 \)
remaining must overlap in exactly 2 positions & need seven of these.

\[
\begin{align*}
\text{IIII} & \text{IO0} \\
\text{0011} & \text{OK} \\
\text{0110} & \\
\text{0101} & \\
\text{1001} & \\
\text{1010} & \\
\text{1100} & \\
\text{1001} & - but one of the above must be duplicated here \text{ (contradiction)}
\end{align*}
\]

Table:

<table>
<thead>
<tr>
<th>wt:</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

must all fall in cases with leader of wt. 2, and two in any one case would violate the minimum distance.

\[\text{can see that this must be in here and is wt. 3 (c.f. argument) copy leader}\]
Note: If \( n \) is not part of the code, we get symmetry through a center point (whereas if \( n \) was there we get symmetry around center line).

Now consider costs of \( w_i \) with 1 word of weight 6, so \( n \) left to spread between 2 and 4.

\[(\overline{3}) = 21 \text{ needed in column 3}\]

But can we have 24 in any of the costs? No.

Note: Any words of \( w_4 \) in the same set must be disjoint (since their sum is a codeword), so at most can have 3 words of \( w_i \) per cost.

\( \Rightarrow \) exactly 3 words of \( w_i \) per cost.

Using symmetry, we complete the table.

<table>
<thead>
<tr>
<th>( w )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Can see \( A(x) = 1 + 7x^3 + 7x^4 + x^7 \)

\( \text{technique important - have all 0's and all 1's in \( 3 \), thus rest in \( 2^3 \), must split evenly) \)

Define: Given \( C \), find \( D \) and \( H \). The code with generator \( H \) (and thus parity-check \( C \)) is called the dual code \( C^\perp \).

- Every code has a unique dual

\[ (C^\perp)^\perp = C \]

- \( C^\perp \) consists of all words \( w \) in the space \( \mathbb{F}_2^m \) such that \( w \cdot x = 0 \), \( x \in C \)

And (MacWilliams Identities)

\( w.e. \) of dual = w.e. of code

Dual of Hamming code is called simplex code.
Dual of \( (n,k) \) has parameters \( (n, n-k) \)

\[ G_{C^\perp} = H_C = \begin{pmatrix}
1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix} \]

Codewords are: \( \mathbf{0000000, r_1, r_2, r_3, 0110110, 1010101, 1100011, 0001111} \).

\[ A_{C^\perp}(x) = 1 + 7x^4 \]
$(7,3,4)$ Simplex Code

$$H_0 = G_0 = \begin{pmatrix}
1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}$$

$$A_0(x) = 1 + 7x^4$$

Given this, how would you work out

wt. enumerators of cosets.

Note that if we add the row $1111111$ to $G_0$, I get a new code, $n=7, k=4$,

wt. enum $= 1 + 7x^3 + 7x^4 + x^7, d=3$

$\Rightarrow$ all 7 columns of $H$ are distinct

$\Rightarrow$ it's a Hamming code $H$.

This is equivalent to our initial $H$

(two codes equivalent if one is column

permutations of $H$ of the other)

$\Rightarrow$ adding overall parity check to $H_0$ gives a code which has only the even
weight codewords of $H_0$

$\Rightarrow G_5 = (7,4,3)$ Hamming code with

odd codewords eliminated.
MacWilliams' Identities (1963)

The weight enumerator of the code is obtained by a linear transformation of the wt. enumerator of the dual code.

Let $B(x) = \text{w.e. of dual} = \sum B_j x^j$, $B_j = \text{no. of codewords of wt. } j$ in $C^\perp$.

$A(x)$ and $B(x)$ are related by

$$B(x) = \frac{1}{2^k} \sum_{j=0}^{\frac{k}{2}} A_j (1-x)^j (1+x)^{n-j}$$

i.e. let $w.e.$ be given as a vector

$$(n,k) A = \begin{bmatrix} A_0 & \ldots & A_n \end{bmatrix} (n+1) \times 1$$

$$(n,n-k) B = \begin{bmatrix} B_0 & \ldots & B_n \end{bmatrix} (n+1) \times 1$$

$$A = B \cdot m \cdot \frac{1}{2}^{n+k}$$

$$B = A \cdot m \cdot \frac{1}{2}^n x$$

$m$ is $(n+1) \times (n+1)$ integer matrix

$$M_{ij} = \begin{cases} \text{coeff} & \text{of } x^j \\ \text{of } x_i & \end{cases}$$

E.g. $(n=4)$

$$a^4 = (1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4$$

$$2 = 1 \cdot (1-x)(1+x)^3 =$$
\[ m = \begin{bmatrix} 1 & 4 & 6 & 4 & 1 \\ 1 & 2 & 0 & -2 & -1 \\ 1 & 0 & -2 & 0 & 1 \\ 1 & -2 & 0 & 2 & -1 \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix} \]

Row sums except first are 0 (good check)

\[ \frac{1}{2^k} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \end{bmatrix} m = \begin{bmatrix} 4 & 0 & 12 & 0 & 0 \end{bmatrix} / 2^k = \begin{bmatrix} 1 & 0 & 3 & 0 & 0 \end{bmatrix} \]

\[ \frac{1}{2^k} \begin{bmatrix} 1 & 0 & 3 & 0 & 0 \end{bmatrix} m = \begin{bmatrix} 4 & 4 & 0 & 4 & 4 \end{bmatrix} / 2^k = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \end{bmatrix} \]

Checking

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

\[ c^T = \]

\[ A = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \end{bmatrix} \]
Mac Williams Identities

\[
A = B \cdot m \cdot \frac{1}{2^{m^2}} \quad \text{and} \quad C = k
\]

\[
B = A \cdot m \cdot \frac{1}{2^k}
\]

In Generator Function Form

\[
B(x) = \frac{1}{2^k} \sum_{i=0}^{\infty} A_i (1-x)^i (1+x)^{n-i}
\]

\[
B(x) = \frac{1}{2^k} \sum_{i=0}^{\infty} A_i m^i
\]

\[
\begin{align*}
\eta_j &= \sum_{i=0}^{\infty} \frac{x^i}{i!} (1-x)^i (1+x)^{n-i} \\
&= \sum_{i=0}^{\infty} (-1)^i \binom{\frac{n}{2}}{i} \binom{\frac{n}{2}-i}{\frac{n}{2}}
\end{align*}
\]

Proof

Need expressions (a) \( \sum_{x \in \mathbb{C}} (-1)^{x \cdot y} \sum_{y \in \mathbb{C}} (-1)^{x \cdot y} \)

Lemma 1

\[
\sum_{x \in \mathbb{C}} (-1)^{x \cdot y} = \begin{cases} 2^k & \text{if } y \in \mathbb{C}^4 \\ 0 & \text{if } y \notin \mathbb{C}^4
\end{cases}
\]

Proof

If \( y \in \mathbb{C}^4 \), then \( x \cdot y = 0 \), \( \forall x \in \mathbb{C} \), \( y \cdot \mathbb{C} = \sum_{x \in \mathbb{C}} (-1)^{x \cdot y} = 2^k \)

If \( y \notin \mathbb{C}^4 \), then \( \exists \) at least one \( x \in \mathbb{C} \) s.t.
\( x \cdot y \neq 0 \) \( \Rightarrow x \cdot y = 1 \). Take any such \( x \) and call it \( x^* \). Now if \( x \cdot y = 0 \), then \( (x+x^*) \cdot y = 1 \) and
if \( x \cdot y = 1 \), then \( (x+x^*) \cdot y = 0 \). By adding \( x^* \)
We divide the code into two: half gives $x \cdot y = 0$, other $x \cdot y = 1$. Thus $\sum_{y \in \mathbb{F}_2} (-1)^{x \cdot y} = 0$.

Lem 2 $\sum_{j \in \mathbb{Z}} (-1)^{x \cdot j} = \omega(x)$ where $j = \omega(x)$, $j$ given.

Proof $x = \underbrace{111\ldots1}_{m-1}00\ldots0$

$y = \underbrace{11\ldots1}_{l}00\ldots0\underbrace{1\ldots1}_{j-l}00\ldots0$

$\Rightarrow (-1)^{x \cdot y} = (-1)^{l}$

$\Rightarrow \sum_{j} (-1)^{x \cdot j} = \sum_{j} (-1)^{l} = \sum_{j} (-1)^{(l \cdot j)} = \omega(x)$

(Krawtchoun coeff)

Main Proof:

$\sum_{x \in \mathbb{F}_2} \sum_{y \in \mathbb{F}_2} (-1)^{x \cdot y} = \sum_{x \in \mathbb{F}_2} \left[ \sum_{y \in \mathbb{F}_2} (-1)^{x \cdot y} \right]$\n
$= 2^k \cdot \beta_j$

$\sum_{x \in \mathbb{F}_2} \sum_{y \in \mathbb{F}_2} (-1)^{x \cdot y} = \sum_{y \in \mathbb{F}_2} m_{x,y}$

$= \sum_{y \in \mathbb{F}_2} A; m_{y,j}$

(since $m_{y,j}$ occurs whenever $x \cdot y = 1$, i.e. $A$; times)

$\Rightarrow \beta_j = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2} A; m_{x,j}$