EHEE 722  Error Correcting Codes

The search for error correcting codes was motivated by Shannon's noisy channel coding theorem of 1948.

Two basic approaches:

I. Algebraic Block Codes
   - Hamming, Slope, Reed-Muller,
   - Bose-Chaudhuri-Hocquenghem, Reed-Solomon

   Encoding and decoding based on theory of cyclic groups.

II. Probabilistic School
   - Shannon, Wozencraft, Fano

   Convolutional Codes and Trellis Codes
   - Sequential decoding, Viterbi decoding,
   - Turbo codes

Block Codes
   - Probabilistic methods computationally complex
   - Chase - suboptimal soft decision decoding
I. Review of linear codes

2.1: Group

- set of elements \( a, b, c, \ldots \) and
- operation \( \cdot \)
  
  1. \( a \cdot b \in G \) for \( a, b \in G \) closure
  
  2. associative law
     \[ a \cdot (b \cdot c) = (a \cdot b) \cdot c \]
  
  3. identity \( e \)
     \[ a \cdot e = e \cdot a = a \]
  
  4. inverse \( a^{-1} \)
     \[ a^{-1} \cdot a = a \cdot a^{-1} = e \]

Def: Abelian Group

- Commutative
  \[ a \cdot b = b \cdot a, \quad a, b \in G \]

Ex.
  1. Addition, integers modulo
     \[ \mathbb{Z}_p \text{ prime } p \]
  2. Multiplication modulo \( p \)
     \[ 1, \ldots, p-1 \]

Def: Field

- set of elements \( a, b, c, \ldots \) two operations \( +, \cdot \)
  
  1. Abelian additive group
  
  2. \( a, b \) elements form Abelian multiplicative group

  3. Distributive Law
     \[ (a + b) \cdot c = a \cdot c + b \cdot c \]
Def. A field with a finite number of elements, \( \mathbb{F}_q \), is called a Galois field and is designated as \( \mathbb{GF}(q) \)

**Linear Codes**

- Information: \( u_3, u_2, u_1 \)
- Encoder: \( \ldots x_3, x_2, x_1 \)
- \( u \)'s and \( x \)'s \( \in \mathbb{GF}(q) \)

**Def. Linear Code**

\[
    x_i = \sum_j u_j \cdot g_{j,i} \quad i = 1, \ldots, \infty
\]

**Arithmetic of \( \mathbb{GF}(q) \)**

**Def. Block Linear Code \( [ (N, K) \text{ code } ] \)**

- Info blocked into groups of \( K \) symbols,
- Code words \( N \) digits,
- Code symbols only depend on corresponding block of \( K \) info symbols.
- Code words:
  \[
  \tilde{x} = [x_1, x_2, \ldots, x_N] \quad \in \mathbb{F}^N \text{ code words}
  \]
- Info:
  \[
  \tilde{u} = [u_1, \ldots, u_K]
  \]
matrix form

\[ [x_1, \ldots, x_k] = [u_1, \ldots, u_k] \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,N} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & & g_{k,N} \end{bmatrix} \]

or

\[ x = uG \]

\[ \uparrow \]

generator matrix

For \( q^k \) distinct code words

\( k \) rows of \( G \) must be linearly independent

Code rate \( R = \frac{k}{N} \) info symbol/codeword

**For:** systematic code

For each info digit appears unaltered in some code word at that digit

**For:** Canonic systematic \((N,K)\) code

First \( K \) code bits are info vector

\( x_i = u_i \) for \( i = 1, \ldots, K \)

**Generator matrix for canonic code**

\[ G = \begin{bmatrix} 1 & 0 & \cdots & 0 & g_{1,K+1} & \cdots & g_{1,N} \\ 0 & 1 & \cdots & 0 & g_{2,K+1} & \cdots & g_{2,N} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & g_{K,K+1} & \cdots & g_{K,N} \end{bmatrix} = [I_k; P] \]
where \( I_k = k \times k \) identity matrix

\[ I \times (N-k) \] matrix

Check Matrix for canonic code

\[ x_i = \sum_{j=1}^{k} u_{i,j} g_{j,i} \quad 1 \leq i \leq N \]

and \( u_{i,j} = x_{i,j} \quad 1 \leq i \leq k \)

so

\[ x_i = \sum_{j=1}^{k} x_{i,j} g_{j,i} \]

For \( k+1 \leq k \leq N \) have \( N-k \) eq's

\[ x_i - \sum_{j=1}^{k} x_{i,j} g_{j,i} = 0 \]

\[ \begin{bmatrix} \delta_{1,k+1} & -\delta_{1,k+2} & \cdots & -\delta_{1,N} \\ -\delta_{2,k+1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots \\ -\delta_{k,k+1} & -\delta_{k,k+2} & \cdots & -\delta_{k,N} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_N \end{bmatrix} = 0 \]

\[ \begin{bmatrix} -P \\ \vdots \\ I_{N-k} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_N \end{bmatrix} = 0 \]

\[ x \cdot H^T = 0 \]
Code words are row space of $G$
Row of $H$ generate $N-K$ dimensional null space of code.

Ternary $(N, K)$ group codes

Code generated by $G_{K \times N}$ of rank $K$

Equivalent to systematic code (not necessarily canonical)
It has some set of code vectors

Proof: Multiple row of $G$ by nonzero constant $\Rightarrow$ same row space
Interchange rows $\Rightarrow$ same space
Add row $\Rightarrow$ same space

\[
\begin{bmatrix}
G_{1,1} & G_{1,2} & \cdots \\
G_{2,1} \\
& \ddots
\end{bmatrix}
\]

Interchange rows so $G_{1,1} \neq 0$
Multiple row $1$ by $G_{1,1}$

\[
\begin{bmatrix}
1 & \cdots \\
G_{2,1} \\
& \ddots
\end{bmatrix}
\]
etc. \rightarrow \text{get the form}

\[ G_{EC} = \begin{bmatrix} 0 & 1 & x & 0 & \cdots & x & 0 & x & \cdots & x \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & x & \cdots & x & 0 & \cdots & x \\ \end{bmatrix} \]

**Permutation Matrix**

\( Q, N \times N \)

rearrangement of identity \( \rightarrow \) nonangular

\( \Rightarrow \) rearrange columns or rows

\[ G_{EC} = [I_k; P] Q \]

\( \downarrow \) echelon canonical

**Check Matrix**

\[ \tilde{X} = \tilde{u} G_{EC} \]

\[ \tilde{X} G^{-1} = \tilde{u} G_{EC} G^{-1} = \tilde{u} [I_k; P] \]

so

\[ \begin{bmatrix} \tilde{u} \\ \tilde{X} G^{-1} \end{bmatrix} \begin{bmatrix} -P \\ \vdots \\ I_{N_k} \end{bmatrix} = 0 \]

so

\[ H^T = Q^{-1} \begin{bmatrix} -P \\ \vdots \\ I_{N_k} \end{bmatrix} \rightarrow H = [I_{N_k}; P] (Q^T)^T \]

\[ \text{Remark: \hspace{1cm} \text{Comment}} \]
Maximum Likelihood Decoding (block codes)

\[ M \text{ code words } = \{ \mathbf{x}_1, \ldots, \mathbf{x}_M \} \]

Receive

\[ \mathbf{y} = (y_1, \ldots, y_N) \]

\[ \begin{array}{c}
\text{ENC} \\
\text{CHANNEL} \\
\text{Reader}
\end{array} \]

\[ \min \ p_e \ (p_e = \text{block error or message error prob}) \]

\[ p_e = \sum_{\mathbf{y}} p(e, \mathbf{y}) = \sum_{\mathbf{y}} \theta(\mathbf{y}) p(e | \mathbf{y}) \]

\[ = \sum_{\mathbf{y}} \theta(\mathbf{y}) \left[ 1 - p(e | \mathbf{y}) \right] \]

\[ p(\mathbf{y}) = \sum_{\mathbf{x}_m} p(\mathbf{x}_m) \theta(\mathbf{y} | \mathbf{x}_m) \text{ only of } m \]

and

\[ \text{only of decision rule} \]

So

\[ \max \ p(e | \mathbf{y}) \]

Decision rule

\[ f(\mathbf{y}) \in \mathcal{C} \]

\[ \mathbf{\hat{x}}_1 \leftarrow \{ \mathbf{\hat{y}}_1 \} \]

\[ \mathbf{\hat{x}}_2 \leftarrow \{ \mathbf{\hat{y}}_3 \} \]

\[ \vdots \]
correct answer if \( \hat{s} \) received and \( \hat{x} = \theta(\hat{s}) \)

transmitted. So decide on \( \hat{x} \) such that

\[
p(\hat{x} \mid \hat{s}) \text{ as max}
\]

\[
\begin{align*}
\text{e. } & P(\hat{x} \mid \hat{s}) \geq P(\hat{x}_i \mid \hat{s}) \quad \text{for } i \neq i' \\
\text{or } & P(\hat{x}_i) P(\hat{s} \mid \hat{x}_i) \geq P(\hat{x}_j) P(\hat{s} \mid \hat{x}_j) \quad \text{if messages equally likely}
\end{align*}
\]

Pick \( \hat{x} \) to max

\[
P(\hat{s} \mid \hat{x})
\]

Maximum likelihood decoding

Special Symmetric, Meanless Channel

Model for equidistant signal set

with white Gaussian noise. - Orthogonal simplex

\[
\begin{align*}
& 1 - \epsilon \\
(1 - \epsilon) \sigma & \quad \text{p (correct plane)} = 1 - \epsilon \\
(1 - \epsilon) \sigma & \quad \text{p (incorrect)} = \sigma \\
(1 - \epsilon) \sigma & \quad (q - 1) \sigma = \epsilon \\
1 - \epsilon & \quad \sigma = \frac{\epsilon}{q - 1}
\end{align*}
\]
Memoryless Channel

\[ P(\tilde{y}_i / x_i) = \prod_{i=1}^n P(y_i / x_i) \]

\[ P(y_i / x_i) = \begin{cases} 1 - \varepsilon & \text{if } y_i = x_i \\ \varepsilon & \text{if } y_i \neq x_i \end{cases} \]

Hamming Distance

\[ d(\tilde{x}, \tilde{y}) = \text{no. of places in which } \tilde{x}, \tilde{y} \text{ differ} \]

so

\[ d(\tilde{x}, \tilde{y}) = N - d(\tilde{x}, \tilde{y}) \]

\[ d(\tilde{x}, \tilde{y}) = \frac{\varepsilon}{\varepsilon - 1} (1 - \varepsilon) \]

\[ d(\tilde{x}, \tilde{y}) = \left[ \frac{\varepsilon}{(1 - \varepsilon)(\varepsilon - 1)} \right] (1 - \varepsilon)^N \]

let \( 0 < \frac{\varepsilon}{(1 - \varepsilon)(\varepsilon - 1)} < 1 \) or \( 0 < \varepsilon < 1 - \varepsilon \)

\[ \varepsilon < \frac{\varepsilon}{(1 - \varepsilon)(\varepsilon - 1)} \Rightarrow P(\text{correct trans. largest}) \]

\[ E < BSC \quad \varepsilon = 2 \quad \text{need } \varepsilon < \frac{1}{2} \]
Then \( P(y|x) \) decreases as \( d(\bar{x}, \bar{y}) \) increase.

So for max. likelihood dec.

such \( \bar{x} \) that is closest to \( \bar{y} \) in

Hamming distance.

Def: weight of vector

\[
w(\bar{x}) = d(\bar{x}, \bar{0})
\]

= number of non-zero components of \( \bar{x} \)

\[\Rightarrow d(\bar{x}, \bar{y}) = w(\bar{x} - \bar{y})\]

**Special Case**  \( GF(2) \)

\[
d(\bar{x}, \bar{0}) = w(\bar{x} + \bar{y})
\]

**EX.** \( \bar{x} = 110111 \)

\( \bar{y} = 101110 \)

\( \bar{x} + \bar{y} = 011001 \)

so \( d(\bar{x}, \bar{y}) = 3 \)

**Distance Between Code Words for \( C(N,K) \) Code**

\[
d(\bar{x}_i, \bar{x}_j) = w(\bar{x}_i - \bar{x}_j)
\]

But \( \bar{x}_i - \bar{x}_j \) is code word

since in linear code sum of 2 code words = c.w.
Proof:

transmit \( \tilde{x} \), receive \( \tilde{y} \)

# error = \( d(\tilde{x}, \tilde{y}) \)

(a) \( H_i \) assume \( 2t+5 < d_{\min} \)

Decoding rule: decode \( \tilde{y} \) to \( \tilde{x}_m \)

if \( d(\tilde{y}, \tilde{x}_m) \leq t \), otherwise say error detected.

notice \( t < \frac{d_{\min}}{2} \)

so sphere of radius \( t \) about code words can't overlap. If \( \tilde{x}_m \) transmitted and # errors \( \leq t \), then \( \tilde{y} \in \mathcal{E}_t(\tilde{x}_m) \) and \( \tilde{x}_m \) decoded correctly. Also \( s < \frac{d_{\min} - 2t}{2} \)

so \( 2t+5 \) errors cannot carry \( \tilde{x}_m \) into

another decoding sphere.

(b) only if: if can correct \( t \) error and detect up to \( t+5 \) errors then \( 2t+5 \leq d_{\min} \)
assume $2t+s \geq d_{\min}$. Let $d(\tilde{x}_i, \tilde{x}_j) = d_{\min}$

assume $t+s \leq d_{\min}$

can find $\tilde{y}$ such that

$$d(\tilde{x}_i, \tilde{y}) \leq t+s$$
$$d(\tilde{x}_j, \tilde{y}) = d_{\min} - (t+s)$$

$$\leq 2t+s - t-s = t$$

so decode to $\tilde{x}_j$ instead of $\tilde{x}_i$, no error.

QED.

Special Case: Error Correction only

to correct $t$ or less errors

all pattern of

$$d_{\min} \geq 2t+1$$
$$\frac{d_{\min} - 1}{2} \geq t$$

detection only if $s < d_{\min}$

Erasures

if decoder not sure of symbol

decide erasure rather than $0, \ldots, q-1$.

So know location but not value.
Proof:
\[ \tilde{x}_i = \tilde{u}_i \cdot G \]
\[ \tilde{x}_j = \tilde{u}_j \cdot G \]

\[ (\tilde{x}_i - \tilde{x}_j) = [\tilde{u}_i - \tilde{u}_j] \cdot G \]

Possible info sequence

Minimum distance, \( d_{\text{min}} \), of code

\[ d_{\text{min}} = \min \{ \text{weight of minimum weight nonzero code word} \} \]

Error correction and detection

(Guaranteed correction/detection Theorem)

Theorem: Given an \((N, K)\) block code, and a channel such that all possible \(N\) tuples can be received given any transmitted code word, then all patterns of \(t\) or fewer errors can be corrected and all patterns of \(t+1, \ldots, t+s\) errors can be detected iff

\[ 2t + s < d_{\text{min}} \quad s, t \geq 0 \]

or \[ 2t + s + 1 \leq d_{\text{min}} \]
Then: \[ d_{\text{min}} \geq 2t + e + 1 \] is a necessary and sufficient condition for correcting \( t \) errors and \( e \) erasures.

**Proof:**

Suff. Assume \( d_{\text{min}} \geq 2t + e + 1 \)

Guess values for erasures. Then \( t \) errors plus at most \( e \) errors from wrong erasure guesses cannot carry \( x \) into another sphere. If no more than \( t \) errors, then can get to only one sphere by substituting values for erasures.

**Necessary:**

Assume \( 2t + e + 1 > d_{\text{min}} \)

Then can get to wrong sphere.

QED.
More on distance structure of $(N,K)$ codes

Then, let $\bar{x}_m$ be any codeword in an $(N,K)$ code $C$. Then for every integer $d$, $0 \leq d \leq N$

$$\# \{ \bar{x} : \bar{x} \in C \text{ and } d(\bar{x}, \bar{x}_m) = d \}$$

$$= \# \{ \bar{x} : \bar{x} \in C \text{ and } w(\bar{x}) = d \}$$

i.e. The number of $\bar{x}$'s of distance $d$ from $\bar{x}_m$ is no. of $\bar{x}$'s of weight $d$

Proof:

$$d(\bar{x}, \bar{x}_m) = w(\bar{x} - \bar{x}_m)$$

as $\bar{x}$ ranges over $C$, $\bar{x} - \bar{x}_m$ ranges over $C$

Proof: for arbitrary group $G$

if $a,b,c,d \in G$, then

$$a + b = c \quad \Rightarrow \quad b = c - a$$

$$a + d = c$$

since $d = b = c - a$

so since $C$ is additive group of $q^K$ elements, for each different $\bar{x} \in C$, $\bar{x} - \bar{x}_m$ is different and as $\bar{x}$ ranges over $C$

all $q^K$ elements generated by $\bar{x} - \bar{x}_m$
so \# of c.w.'s distance \( d \) from \( \hat{x}_m \) =
\# of c.w.'s of weight \( d \).

Q.E.D.

Comment: This says that if one stands on a codeword in an \((N,K)\) code and looks out at the other codewords, then one sees the same set of distances regardless of the codeword chosen as the vantage point.

Properties of \( H \)

Given code \( C \) with parity check matrix \( H \).

Then
\[ \hat{x} H^T = 0 \quad \text{for} \quad \hat{x} \in C \]

Lemma:

Every codeword \( \hat{x} \) specifies a linearly dependent set of \( W(\hat{x}) \) columns of \( H \).

Conversely, a linear combination of \( w \) columns of \( H \) equal to \( \hat{o} \) specifies a codeword of weight \( w \).

Average Hamming Distance for \((N,K)\) Codes

Lemma: Let \( G \) be the generator matrix of an \((N,K)\) code and \( n_i(x) = \# \{ \hat{x} : \hat{x} \in C \text{ and } x_i = x \} \)
Then if $i$th column of $G$ is not all 0,

$$h_i(x) = x^{k-1}$$

for every $x \in GF(q)$

Proof:

$$x_i = \sum_{j=1}^{k} u_j g_{ij}$$

assume $g_{1i} \neq 0$

$$x_i = g_{1i} u_1 + \sum_{j \neq 1} u_j g_{ji}$$

For each of $q^{k-1}$ possible sequences $(u_1, \ldots, u_{k-1}, u_{k+1}, \ldots, u_k)$

only one $u_1$ such that $x_i = 0$

Q.E.D.

If $i$th column of $G$ is $0$, then $x_i = 0$

for all code words. Call this an idle position and use $N'$ as number of non-idle positions.

Theorem:

For any $(N,k)$ code with $N'$

non-idle positions

$$d_{av} = N' (q-1) \frac{q^{k-1}}{q^k - 1} \geq q^{k-1} N'$$
where
\[ d_{avg} = \frac{\sum \text{distances to other code words}}{\text{number of other code words}} \]

\[ = \sum_{i \neq j} d(\bar{x}_i, \bar{x}_j) \]
\[ \sum_{i \neq j} \]
\[ q - 1 \]

Proof:
\[ d_{avg} = \sum_{\bar{x} \neq 0} \sum_{k=0}^{q-1} w(\bar{x}) \]

Code word array

\[
\begin{align*}
\bar{x}_1 & = x_1, x_2, \ldots, x_N \\
\bar{x}_2 & = x_2, x_2, \ldots, x_N \\
& \vdots \\
\bar{x}_k & = x_k, x_k, \ldots, x_k, x_N \\
\bar{x}_{q-1} & = x_1, x_1, \ldots, x_1, x_N \\
\end{align*}
\]

\[ \sum_{\bar{x} \neq 0} w(\bar{x}) = \text{number of codes with nonzero component} \]

Pick nonzero column

each of \( q-1 \) nonzero elements

appear \( q^{k-1} \) times in column

so column weight is \((q-1)q^{k-1}\) for each
nonidle column, so $\sum \psi(x) = N'(q - 1/2 q^{k-1})$

Q.E.D.

Upper bound on $d_{\text{min}}$

Theorem:

$$d_{\text{min}} \leq d_{\text{avg}} = \beta', q^{k-1} \frac{q-1}{q^{k-1}}$$

 Syndrome Decoding (Ref: Gallager - 6.1)

 Transmit $\tilde{x}$

 Receive $\tilde{y} = \tilde{x} + \tilde{z}$

 Syndrome $\tilde{s} = \tilde{y}H^T = \tilde{z}H^T + \tilde{x}H^T = \tilde{z}H^T$

 Set has $q^k$ solutions $\{\tilde{z}_{\text{actual}} + \tilde{x}_i\}_{i=1}^{q^k}$

 For more likelihood decoding choose minimum weight solution for special symmetric channel discussed above or most likely solution in general

 Decoding Table

 List of syndromes and corresponding most likely error patterns have $q^{N-k}$ possible syndromes.
EXAMPLE

Channel: Bsc, crossover \( e < \frac{1}{2} \)

\[ \begin{array}{c|c|c|c|c|c|c|c} 
H & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
T & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
\end{array} \]

Error \( \tilde{z} \)

\( \begin{array}{c|c|c} 
5 & 0 & 0 \\
3 & 0 & 1 \\
5 & 0 & 1 \\
6 & 1 & 0 \\
4 & 0 & 1 \\
7 & 1 & 1 \\
\end{array} \)

Decoding Table

Decide to \( \hat{z} = \tilde{y} - \tilde{z} \)

Comment: Only error patterns in decoding table are decoded correctly. Any other error would give a syndrome in table and be decoded to wrong pattern.

Probability of block error in decoding:

From table all 6 single error patterns and 1 double error pattern correctable.

\[ P_e = 1 - P_c = 1 - (1-e)^6 - 6 e (1-e)^5 - e^2 (1-e)^4 \]

Note: \( d_{min} = 3 \) since 3 checked rows add to (000)
Block diagram of Syndrome Decoder

\[ \begin{array}{c}
\bar{y} \\
\downarrow \\
H^T \\
\downarrow \\
f(s) \\
\downarrow \\
N^* \\
\downarrow \\
\bar{x} \\
\end{array} \]

\( f(s) \) is a logic block that generates \( \bar{x} \) for given \( s \). For long codes, \( f(s) \) very complex. \( N-K \) computations will look for simpler decoders to implement.

Comment: Syndrome decoding takes full advantage of distance structure of code. Can correct some error patterns of weight \( \geq \text{min} \{d\} \).

Def: Perfect Code

A code is said to be perfect if it can correct all error patterns of weight \( t \) or less and no others.

Lemma: Relation between number of syndromes and number of code words

Let \( a = \) number of syndromes = \( v \) of correctable error patterns

\( b = \) number of possible received words
Then the number of information symbols is

\[ K = \log_2 \frac{b}{a} \]

Proof: For \((N, K)\) code \(a = 2^t\), \(b = 2^N\)

Q.E.D.

Theorem: A necessary condition for the existence of a perfect \((N, K)\) binary code that corrects up to \(t\) errors is

\[ a = \sum_{i=0}^{N-K} \binom{N}{i} = 2^{N-K} = \#\text{ syndromes} \]

Proof:

The left hand side is the number of error patterns of weight \(t\) or less. If \(a \neq 2^{N-K}\), then can't have \(2^k\) code words.

Q.E.D.

Examples of Linear Codes (Petersen - Ch. 5)

1. Binary Hamming Single-Error Correcting Codes

\( H \) is \( m \times (2^m - 1) \) matrix whose columns are all possible \(2^m - 1\) non-zero binary vectors of length \(m\)

So \( N = 2^m - 1 \), \( N - K = m \)

\[ (2^m - 1, 2^m - m - 1) \text{ code} \]
can correct all single errors.

Proof: assume error in $i$th position

Then $s_i^T = i$th column of $H$.

All columns of $H$ unique so syndrome gives error location.

also can't correct more than 1 error since sum of two columns

of $H$ = another column $\Rightarrow$ wrong correction.

so $d_{\min} \geq 3$

Lemma: For this code $d_{\min} = 3$

Proof: for $n > 1$ the following $3$ columns are always linearly dependent

$$m \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ \vdots & \vdots & \vdots \\ 0 & 1 & 1 \end{vmatrix}$$

Q.E.D.

code rate

$$R = \frac{m}{2^m - 1} = 1 - \frac{m}{2^m - 1}$$

$$\lim_{m \to \infty} R = 1$$
So for binary channel, cannot make $P_e \to 0$ by increasing $N$ since $c < 1$

Notice that these are perfect codes.

Ex: $(7, 4)$ code

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

2. Binary Hamming single error correcting 2 error detecting codes

Add overall parity check to previous code to form $(2^m, 2^{m-1} - 1)$ code.

i.e. let $x = \sum x_i \mod 2^{n+1}$ so new

Check matrix is

\[
H_2 = \begin{bmatrix}
1 & 0 & 1 & \cdots & 1 & 0 \\
1 & 1 & \cdots & 1 & 1
\end{bmatrix}_{2 \times 2^{m-1}}
\]

For even weight code words $X_{n+1} = 0$.

"odd" $X_{n+1} = 1$

So all $x$ have even weight.

$\Rightarrow d_{\text{min}} = 4$

Decoding scheme:

1. If $\hat{e} = 0$ decide no error

2. If $A_{n+1} = 1$ and $e_{n+1} = m \neq 0$
decide single error and \( x_1, \ldots, x_m \)
gives location, if \( \{ x_1, \ldots, x_m \} = 0 \) decide \( x_{n+1} \) in even.
3. If \( x_{n+1} = 0 \), \( \{ x_1, \ldots, x_m \} \neq \emptyset \)
detect error (weight must be even)

Hamming codes can be generalized
to \( \text{GF}(p) \) where \( p \) is a prime no.
See - Peterson Ch.5 (also gives
formula for the number of code
words of each weight)

3. Repetition Code
\((N,1)\) code
\[ 1 \rightarrow (1, \ldots, 1) \]
\[ 0 \rightarrow (0, \ldots, 0) \]
For \( N \) odd can correct \( \frac{N-1}{2} \) errors
by taking majority vote.
Perfect code
\[ R = \frac{1}{N} \]
\[ \lim_{N \to \infty} R = 0 \] so get reliable
transmission of practically no data

4. Maximal Length Codes
Let \( A_m \) denote a matrix over
\( \text{GF}(q) \) of dimension \( m \times (q^m-1) \)
whose columns are all the distinct
non-zero m-tuples.

Theorem: an \((N, k)\) code with
\[
G = A_k
\]
is an equidistant code
having \(d_{\text{min}} = d_{\text{avg}} = (q-1) q^{k-1}\)
and \(N = q^{k+1}\). Each non-zero

codeword contains each non-zero

element of \(GF(q)\) in exactly
\(q^{k-1}\) positions.

Proof: let \(\mathbf{w} = (w_1, \ldots, w_k)\) be
any non-zero information vector
and suppose that \(\mathbf{w} \neq \mathbf{0}\). Then

\[
x_i = g_i \mathbf{w} + \sum_{j \neq i} g_{ij} w_j
\]

\(i \neq k\)

Keep \(\mathbf{w}\) fixed but vary \(i\). Since
all non-zero \(q^{k-1}\) \(k\)-vectors for
\((g_{i1}, \ldots, g_{ik})\) occur, all \(q^{k-1}\)
possibilities for \((g_{i1}, g_{i2}, g_{i3}, g_{i4}, \ldots, g_{ik})\)

occur. For any \(j \neq \mathbf{w} \in GF(q)\), there
is only one choice for \(g_{ij}\) to make
\(x_i = \mathbf{w}\) for each of \(q^{k-1}\) choices
of other \(g_{ij}\). Therefore \(\mathbf{w}\) occurs
exactly \(q^{k-1}\) times in each code word.

Note: Reason for requiring \(a \neq 0\)

\(g_{2i} = (g_{1i}, g_{k+1}, g_{k+1}, \ldots, g_{k+1}, g_{k+i}) = \mathbf{0}\)
can occur. Then

\(g_{1i} = (g_{1i}, g_{k+1}, g_{k+1}, \ldots, g_{k+1}, g_{k+i}) = \mathbf{0}\)
\[ w(x) = (q - 1)^{k-1} \]

From (22) \[ d_{\text{min}} = (q^k - 1) \frac{q^{k-1} - (q-1)}{q-1} = (q-1)^{k-1} \]

One of Hamming Bound

Def. Dual Codes

Two linear codes are duals if the generator matrix for one is the parity check matrix for the other.

Ex. Let \( q = 2 \), then the 6 for maximal length codes is 11 for Hamming single error correcting code.

5. Golay \((23, 12)\) code

\[ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 1 & 1 & 1 & 1 \end{pmatrix} \]

⇒ perfect \((23, 12)\) code

might exist. Will show latter as a BCH code

Hamming, Repetition, + Golay are only known perfect binary codes!

II. Bounds on Error Correction Capabilities of Block Codes