ENEE 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, Slepian, Reed-Muller, Bose-Chaudhuri-Hoquenghem, 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

Def.: 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

$$a \cdot b = b \cdot a \quad \forall \; a, b \in G$$

EX. (1) addition, integers modulo p a prime no.

(2) mult. modulo p

$$1, \ldots, p-1$$

Def: Field

Set of elements, two operations $+, \cdot$

(1) abelian additive group

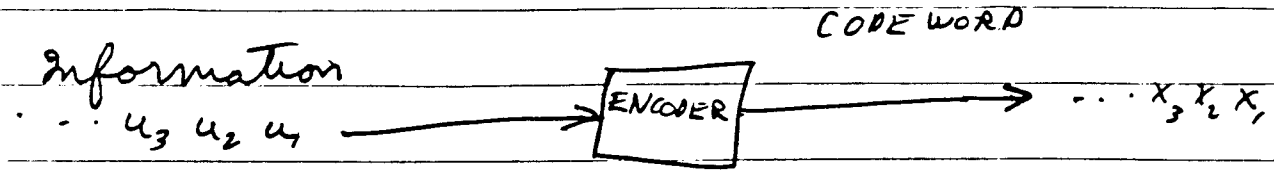
(2) non 0 elements form abelian multiplicative group

(3) Distributive Law

$$(a+b) \cdot c = a \cdot c + b \cdot c$$

Def: A field with a finite number of elements, q, is called a Galois field and is designated as $GF(q)$

Linear Codes



u's and x's $\in GF(q)$

Def: Linear Code

$$x_i = \sum_j u_j\, g_{ji} \qquad i = 1, \cdots \infty$$

arithmetic of $GF(q)$

Def: Block Linear Code [(N, K) group 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

$\vec{x} = [x_1, x_2, \cdots x_N]$ — q^K code words

Info $\vec{u} = [u_1, \cdots, u_K]$

Matrix form

$$[x_1, \dots x_N] = [u_1, \dots u_K] \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,N} \\ g_{2,1} & \vdots & & \vdots \\ \vdots & & & \\ g_{K,1} & g_{K,2} & & g_{K,N} \end{bmatrix}$$

or

$$\vec{x} = \vec{u}\ G$$

generator matrix

For q^K distinct code words
K rows of G must be linearly indepen

Code Rate $R = \frac{K}{N}$ $\frac{\text{info symb}}{\text{code symbol}}$

Def: Systematic Code
~~for~~ Each info digit appears
unaltered ~~as~~ ~~some~~ code word ~~dot~~ digit

Def: Canonic Systematic (N,K) code
First K code bits are info vector
$x_i = u_i$ for $i = 1, \dots, K$

Generator matrix for canonic code

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & g_{1,K+1} & \cdots & g_{1,N} \\ 0 & 1 & & \vdots & g_{2,K+1} & & \vdots \\ \vdots & \vdots & & & \vdots & & \\ 0 & 0 & \cdots & 1 & g_{K,K+1} & \cdots & g_{K,N} \end{bmatrix} = [I_K \mid P]$$

where I_k = $k \times k$ identity matrix

P = $k \times (N-k)$ matrix

Check Matrix for canonic code

$$x_i = \sum_{j=1}^{k} u_j g_{ji} \qquad 1 \le i \le N$$

and $u_i = x_i \qquad 1 \le i \le k$

so

$$x_i = \sum_{j=1}^{k} x_j g_{ji}$$

For $k+1 \le i \le N$ have $N-k$ eq's

$$x_i - \sum_{j=1}^{k} x_j g_{ji} = 0$$

or

$$[x_1, \dots x_N] \begin{bmatrix} -g_{1,k+1} & -g_{1,k+2} & \cdots & -g_{1,N} \\ -g_{2,k+1} & \vdots & & \vdots \\ \vdots & & & \vdots \\ -g_{k,k+1} & -g_{k,k+2} & & -g_{k,N} \\ +1 & 0 & & 0 \\ 0 & 1 & & 0 \\ \vdots & 0 & & \vdots \\ 0 & 0 & & 1 \end{bmatrix} = \vec{0}$$

or

$$\vec{x} \underbrace{\begin{bmatrix} -P \\ \hline I_{N-k} \end{bmatrix}}_{H^T} = 0$$

or

$$\vec{x} H^T = \vec{0}_{1 \times (N-k)}$$

Code words are row space of G

Rows of H generate N-K dimensional null space of code.

Arbitrary (N, K) Group Codes

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

equivalent to systematic code (not necessarily canonic)

i.e. has same set of code vectors

Proof: mult. row of G by nonzero constant $\Rightarrow$ same row space

interchange rows $\Rightarrow$ same space

add rows $\Rightarrow$ same space

$$\begin{bmatrix} g_{1,1} & g_{1,2} & \cdots \\ g_{2,1} & & \\ \vdots & & \end{bmatrix}$$

Interchange rows so $g_{1,1} \neq 0$

~~Divide~~ mult. row 1 by $g_{1,1}^{-1}$,

$$\begin{bmatrix} 1 & \cdots \\ g_{2,1} & \\ \vdots & \end{bmatrix}$$

etc. $\rightarrow$ get to form

$$G_{EC} = \begin{bmatrix} 0 & 1 & x & 0 & x & \cdots & x & 0 & x & \cdots & x \\ 0 & 0 & 0 & 1 & x & & x & & x & & x \\ \vdots & 0 & & 0 & 0 & & & & & & \vdots \\ & & & & & & & 0 & x & & \\ 0 & 0 & 0 & 0 & 0 & & 0 & 1 & x & & x \end{bmatrix}$$

Permutation Matrix

Q, $N \times N$

rearrangement of identity $\Rightarrow$ nonsingular

$\Rightarrow$ rearranges columns or rows

$$G_{EC} = [I_K \mid P]\, Q$$

$\rightarrow$ echelon canonic

<u>Check Matrix</u>

$$\vec{x} = \vec{u}\, G_{EC}$$

$$\vec{x}\, Q^{-1} = \vec{u}\, G_{EC} Q^{-1} = \vec{u}\, [I_K \mid P]$$

so

$$\vec{x}\, Q^{-1} \begin{bmatrix} -P \\ \hline I_{N-K} \end{bmatrix} = 0$$

so

$$H^T = Q^{-1} \begin{bmatrix} -P \\ \hline I_{N-K} \end{bmatrix} \Rightarrow H = [-P^T \mid I_{N-K}]\,(Q^{-1})^T$$

<u>Remark</u>: ~~Ground~~

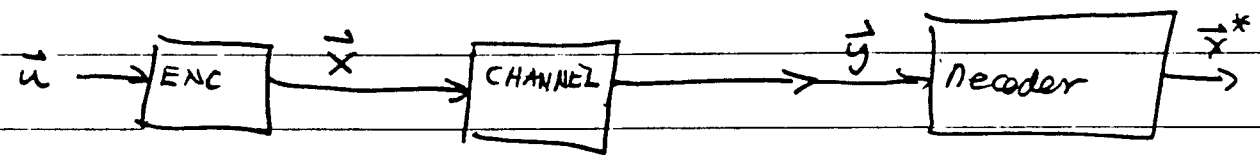
Maximum Likelihood Decoding (Block codes)

M code words

$$\vec{x}_i = (x_{i1}, \dots x_{iN}), \quad i = 1, \dots M \qquad \mathcal{C} = \{\vec{x}_i ; i = 1, \dots, M\}$$

Receive

$$\vec{y} = (y_1, \dots y_N)$$



min P_e (P_e = block error or message error prob)

$$P_e = \sum_{\vec{y}} P(e, \vec{y}) = \sum_{\vec{y}} P(\vec{y}) P(e/\vec{y})$$

$$= \sum_{y} P(\vec{y}) [1 - P(c/\vec{y})]$$

$$P(\vec{y}) = \sum_{m} P(\vec{x}_m) P(\vec{y}/\vec{x}_m)$$ indep of m

and indep of decision rule

so $\max P(c/\vec{y})$

decision rule

$f(\vec{y}) \in \mathcal{C}$

$\vec{x}_1 \longleftarrow \{ \vec{y}_1, \dots, \vec{y}_j$

$\vec{x}_2 \longleftarrow \{$

$\vdots$

correct decision if $\vec{y}$ received and $\vec{x} = f(\vec{y})$ transmitted. So decide on $\vec{x}$ such that

$$P(\vec{x}/\vec{y}) \text{ as max}$$

i.e.

$$P(\vec{x}_i/\vec{y}) \geq P(\vec{x}_j/\vec{y}) \quad \text{for } j \neq i$$

or

$$P(\vec{x}_i)\,P(\vec{y}/\vec{x}_i) \geq P(\vec{x}_j)\,P(\vec{y}/\vec{x}_j) \quad j = i$$

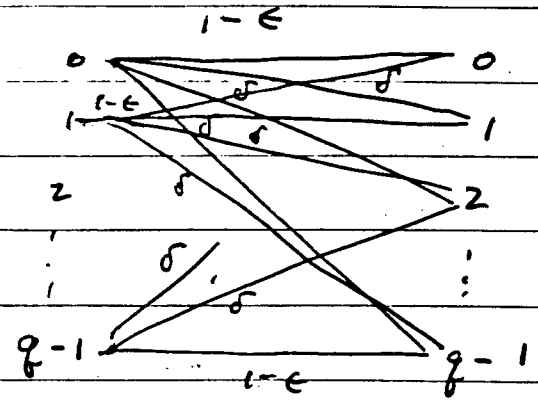
If messages equally likely

$\Rightarrow$

$$\boxed{\begin{array}{c}\text{Pick } \vec{x} \text{ to max} \\ P(\vec{y}/\vec{x}) \\ \text{Maximum likelihood Decoding}\end{array}}$$

Special Symmetric, Memoryless Channel

Model for equidistant signal sets with white Gaussian noise. — orthogonal, simplex



$P(\text{correct trans}) = 1 - \epsilon$

$P(\text{incorrect}) = \delta$

so $(q-1)\delta = \epsilon$

or $\delta = \dfrac{\epsilon}{q-1}$

Memoryless channel

$$P(\vec{y}/\vec{x}) = \prod_{i=1}^{N} P(y_i/x_i)$$

$$P(y_i/x_i) = \begin{cases} 1-\epsilon & \text{if } y_i = x_i \\ \delta & \text{if } y_i \neq x_i \end{cases}$$

Hamming Distance

$d(\vec{x}, \vec{y})$ = no. of places in which $\vec{x}, \vec{y}$ differ

so $$P(\vec{y}/\vec{x}) = \delta^{d(\vec{x},\vec{y})} (1-\epsilon)^{N-d(\vec{x},\vec{y})}$$

$$= \left(\frac{\epsilon}{q-1}\right)^{d(\vec{x},\vec{y})} (1-\epsilon)^{N-d(\vec{x},\vec{y})}$$

$$= \left[\frac{\epsilon}{(1-\epsilon)(q-1)}\right]^{d(\vec{x},\vec{y})} (1-\epsilon)^{N}$$

let $0 < \dfrac{\epsilon}{(1-\epsilon)(q-1)} < 1$ or $\delta = \dfrac{\epsilon}{q-1} < 1-\epsilon$

or $\epsilon < \dfrac{q-1}{q} \Rightarrow$ P(correct trans. largest)

Ex - BSC $q=2$ need $\epsilon < \frac{1}{2}$

Then

$P(\vec{y}/\vec{x})$ decreases as $d(\vec{x},\vec{y})$ increases

so for max. likelihood dec.

Pick $\vec{x}$ that is closest to $\vec{y}$ in Hamming distance.

<u>Def: weight of vector</u>

$$w(\vec{x}) = d(\vec{x},\vec{0})$$

$$= \text{number of nonzero components of } \vec{x}$$

$$\Rightarrow \quad d(\vec{x},\vec{y}) = w(\vec{x}-\vec{y})$$

<u>Special Case GF(2)</u>

$$d(\vec{x},\vec{y}) = w(\vec{x}+\vec{y})$$

EX. $\vec{x} = 110111$

$\vec{y} = 101110$

$\vec{x}+\vec{y} = 011001$

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

<u>Distance Between Code Words for (N,K) Code</u>

$$d(\vec{x}_i,\vec{x}_j) = w(\vec{x}_i - \vec{x}_j)$$

but $\vec{x}_i - \vec{x}_j$ is code word

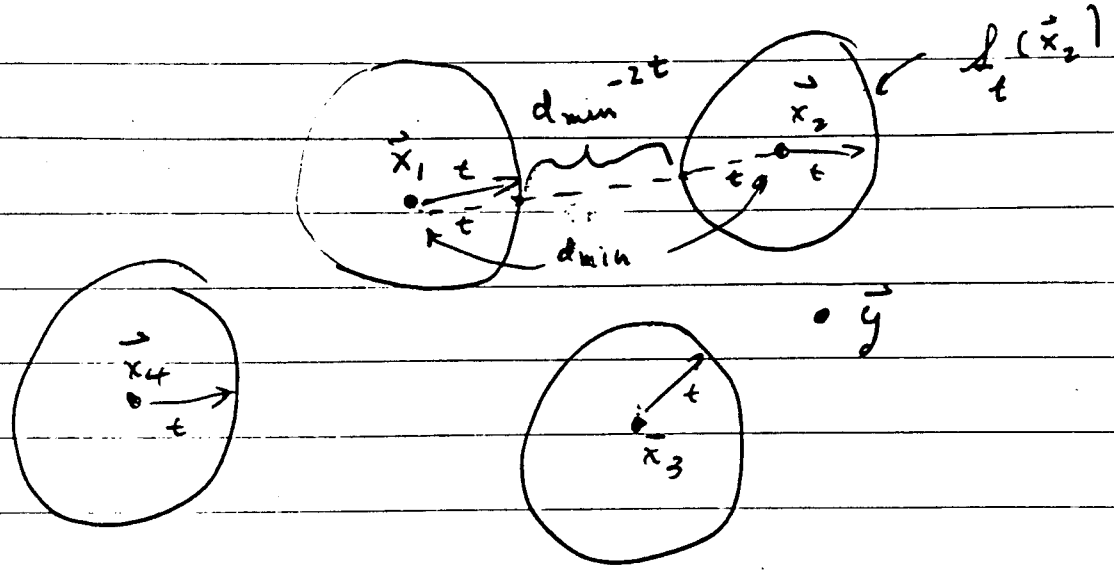
since in linear code sum of 2 code words = c.w.

Proof:

transmit $\vec{x}$, receive $\vec{y}$

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

(a) (H) assume $2t+s < d_{min}$



Decoding rule: decode $\vec{y}$ to $\vec{x}_m$ if $d(\vec{y}, \vec{x}_m) \leq t$, otherwise say error detected.

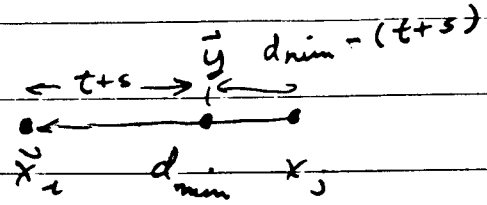
notice $t < \frac{d_{min}}{2}$, $\Rightarrow$ ~~sphere sets~~

so spheres of radius t about code words can't overlap. If $\vec{x}_m$ transmitted and $\#$ errors $\leq t$, then $\vec{y} \in S_t(\vec{x}_m)$ and is decoded correctly. also $s < d_{min} - 2t$ so $t+1, \ldots t+s$ errors cannot carry $\vec{x}_m$ into another decoding sphere.

(b) <u>Only if</u>: If can correct up to t error and detect up to $t+s$ errors then $2t+s < d_{min}$

Assume $2t+s \geq d_{min}$. Let $d(\vec{x}_i, \vec{x}_j) = d_{min}$

Assume $t+s \leq d_{min}$ errors



can find $\vec{y}$ such that

$$d(\vec{x}_i, \vec{y}) \leq t+s$$
$$d(\vec{x}_j, \vec{y}) = d_{min} - (t+s)$$
$$\leq 2t+s-t-s = t$$

So decode to $\vec{x}_j$ instead of $\vec{x}_i$ + make error

QED.

Special Case: <u>Error Correction only</u>

to correct all patterns of t or less errors

$$\boxed{d_{min} \geq 2t+1} \quad \text{or} \quad \frac{d_{min}-1}{2} \geq t$$

Detection only $t=0$
$s < d_{min}$

<u>Erasures</u>

If decoder not sure of symbol decide erasure rather than $0, \cdots, q-1$. So know location but not value,

Proof:

$$\vec{x}_i = \vec{u}_i G$$

$$\vec{x}_j = \vec{u}_j G$$

$$(\vec{x}_i - \vec{x}_j) = \underbrace{[\vec{u}_i - \vec{u}_j]}_{\text{possible Info sequence}} G$$

<u>Minimum Distance, d_{min}, of Code</u>

$$d_{min} = \min_{\substack{i,j \\ i \neq j}} w(\vec{x}_i - \vec{x}_j)$$

= weight of minimum weight, non zero, code word

<u>Error correction and Detection</u>

(Guaranteed correction + detection Thm)

<u>Thm</u>: Given an (N,K) block code with minimum Hamm distance d_{min}, 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 $t+1, \cdots, t+s$ errors can be detected iff

$$2t + s < d_{min} \qquad s, t \geq 0$$

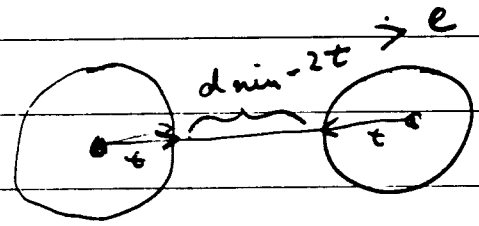
or $\quad 2t + s + 1 \leq d_{min}$

Thm.

$d_{min} \geq 2t + e + 1$ is a necessary + sufficient condition for correcting t errors and e erasures.

<u>Proof:</u>

Suff. assume $d_{min} \geq 2t + e + 1$



guess values for erasures, then t errors + at most e errors from wrong erasure guesses can not ~~carry~~ carry $\vec{x}$ into another sphere. If no more than t errors, then can get to only one sphere by substituting values for erasures.

<u>Necessary:</u>

Assume $2t + e + 1 > d_{min}$

Then can get to wrong sphere

QED.

More on distance structure of (N, K) codes

<u>Thm.</u> Let $\vec{x}_m$ be any codeword in an (N, K) code $\mathcal{C}$. Then for every integer d, $0 \le d \le N$

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

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

i.e. The number of c.w.'s of distance d from $\vec{x}_m$ = no. of c.w's of weight d

Proof:

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

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

Proof: for arbitrary group $\mathcal{G}$

if $a, b, c, d \in \mathcal{G}$, then

$$\left.\begin{array}{l} a + b = c \\ a + d = c \end{array}\right\} \Longrightarrow b = d$$

since $d = b = c - a$

so since $\mathcal{C}$ is additive group of q^K elements, for each different $\vec{x} \in \mathcal{C}$, $\vec{x} - \vec{x}_m$ is different and as $\vec{x}$ ranges over $\mathcal{C}$ all q^k elements generated by $\vec{x} - \vec{x}_m$

so # of c.w's distance d from $\vec{x}_m$ $\supset$ no. of c.w's of weight d.

QED.

<u>Comment:</u> Thm. 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.

<u>Properties of H</u>

Given code $\mathcal{C}$ with parity check matrix H

Then

$$\vec{x} H^T = \vec{0} \qquad \text{for } \vec{x} \in \mathcal{C}$$

<u>Lemma</u>

Every codeword $\vec{x}$ specifies a linearly dependent set of $w(\vec{x})$ columns of H. Conversely, a linear combination of w columns of H equal to $\vec{0}$ specifies a codeword of weight w.

<u>Average Hamming Distance for (N,K) Codes</u>

<u>Lemma</u>: Let G be the generator matrix of an (N,K) code and $n_i(\alpha) = \#\{\vec{x} : \vec{x} \in \mathcal{C} \text{ and } x_i = \alpha\}$

Then if i^{th} column of G is not all 0,

$$n_i(\alpha) = q^{k-1} \quad \text{for every } \alpha \in GF(q)$$

Proof:

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

assume $g_{\ell i} \neq 0$

$$x_i = g_{\ell i} u_\ell + \sum_{j \neq \ell} u_j g_{ji}$$

For each q^{k-1} possible sequences

$$(u_1, \dots u_{\ell-1}, u_{\ell+1}, \dots u_k)$$

only one u_ℓ such that $x_i = \alpha$

QED.

If i^{th} column of G is $\vec{0}$, then $x_i = 0$ for all code words. Call this an idle position and use N' as number of non-idle positions.

<u>Theorem</u>:

For any (N,k) code with N' non-idle positions

$$d_{avg} = N'(q-1)\frac{q^{k-1}}{q^k-1} \cong \frac{q-1}{q} N'$$

where

$$d_{avg} = \frac{\sum \text{ distances to other code words}}{\text{number other code words}}$$

$$= \frac{\sum_{\substack{i \\ i \neq j}} d(\vec{x}_i, \vec{x}_j)}{q^K - 1}$$

Proof:

$$d_{avg} = \frac{\sum_{\vec{x} \neq 0} w(\vec{x})}{q^K - 1}$$

Code word array

$$\begin{array}{lcllll}
\vec{x}_1 & = & x_{11} & x_{12} & \cdots & x_{1N} \\
\vec{x}_2 & = & x_{21} & x_{22} & \cdots & x_{2N} \\
\vdots & = & \vdots & & & \vdots \\
\vec{x}_{q^K-1} & = & x_{q^K-1,1} & & \cdots & x_{q^K-1,N}
\end{array}$$

$\sum_{\vec{x} \neq 0} w(\vec{x})$ = number of slots with nonzero component

Pick non idle column

each of $q-1$ nonzero elements appears q^{K-1} times in column

so column weight is $(q-1)\, q^{K-1}$ for each

non idle column. So $\sum_{\vec{x} \neq 0} w(\vec{x}) = N'(q-1)q^{K-1}$

Q.E.D.

Upper bound on d_{min}

Theorem:

$$d_{min} \leq d_{avg} = N' q^{K-1} \frac{(q-1)}{q^K - 1}$$

- Syndrome Decoding (Ref: Gallager - 6.1)

Transmit $\vec{x}$

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

Syndrome

$$\vec{s} = \vec{y} H^T = \vec{z} H^T + \cancel{\vec{x} H^T}^{\,0} = \vec{z} H^T$$

Set has q^K solutions $\{ \vec{z}_{actual} + \vec{x}_i \}_{i=1}^{q^K}$

For max. 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 pattern. Have q^{N-K} possible syndromes.

EXAMPLE

Channel: BSC, crossover $\epsilon < 1/2$

	H^T	Error $\vec{z}$	$\vec{s}$	
	$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	000 000	000	0
		100 000	011	3
✓		010 000	101	5
✓		001 000	110	6
✓		000 100	100	4
		000 010	010	2
		000 001	001	1
		~~110 000~~	~~110~~	
		~~101 000~~	~~101~~	
		100 100	111	7

Decoding Table

decode to $\vec{x} = \vec{y} - \vec{z}$

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.

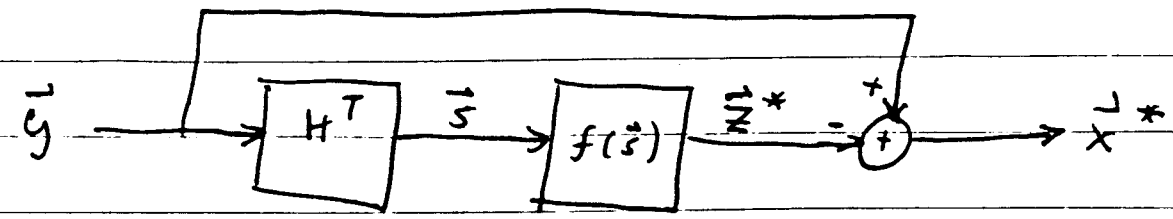
Probability of block error in decoding:

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

$$P_e = 1 - P_c = 1 - (1-\epsilon)^6 - 6\,\epsilon\,(1-\epsilon)^5 - \epsilon^2(1-\epsilon)^4$$

Note: $d_{min} = 3$ since 3 checked rows add to (000)

Block Diagram of Syndrome Decoder



$f(\vec{s})$ is a logic block that generates $\vec{z}$ for given $\vec{s}$. For long codes $f(\cdot)$ very complex $\sim q^{N-K}$ 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 $> d_{min}/2$

Def: Perfect Code

a codes is said to be perfect if it can correct all error patterns of weight t or less and no others.

<u>Lemma</u>: Relation between number of syndromes and number of code words

Let a = number of syndromes = no. of correctable error patterns

b = number of possible received words

Then the number of info. symbols is

$$K = \log_q \frac{b}{a}$$

Proof: For (N, K) code $a = q^{N-K}$, $b = q^N$

Q.E.D.

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

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

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.

QED.

<u>Examples of Linear Codes</u> (Peterson - 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 ~~vec~~ vectors of length m

so $N = 2^m - 1$, $N - K = m$

$\Rightarrow$ $(2^m - 1, 2^m - m - 1)$ code

can correct all single errors.

Proof: assume error in i^{th} position

Then $\vec{s}^T = i^{th}$ 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 $m > 1$ the following 3 columns are always linearly dependent

$$m \left\{ \begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ \vdots & \vdots & \vdots \\ 0 & 1 & 1 \end{matrix} \right.$$

Q.E.D.

Code rate

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

$$\lim_{m \to \infty} R = 1$$

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

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

2. Binary Hamming single error correcting 2 error detecting codes

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

i.e. let $x_{N+1} = \sum_{i=1}^{N} x_i$. So new

check matrix is

$$H_1 = \begin{array}{c} \leftarrow 2^m - 1 \rightarrow \\ \left[\begin{array}{ccc|c} H & & & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 1 & 1 & 1 \cdots 1 & 1 \end{array}\right] \end{array} \begin{matrix} \downarrow \\ m \\ \uparrow \end{matrix}$$

For even weight code words in original code, $x_{N+1} = 0$

" odd " " " , $x_{N+1} = 1$

So all $\vec{x}$ have even weight

$\Longrightarrow d_{min} = 4$

- Decoding scheme:

1. If $\vec{s} = \vec{0}$ decide no error
2. If $s_{m+1} = 1$ and $\{s_1, \ldots s_m\} \neq 0$

decide single error and $[s_1, \dots, s_m]$ gives location, if $(s_1, \dots, s_m) = 0$ decide x_{N+1} in error

3. If $s_{m+1} = 0$, $[s_1, \dots, s_m] \neq \vec{0}$ detect error (weight must be even)

Hamming codes can be generalized to $GF(p)$ 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

$1 \longrightarrow (1, \dots 1)$

$0 \longrightarrow (0, \dots, 0)$

For N odd can correct $\leq \frac{N-1}{2}$ 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 $GF(q)$ 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 $d_{min} = d_{avg} = (q-1)\, q^{K-1}$ and $N = q^K - 1$. Each non-zero codeword contains each <u>non-zero</u> element of $GF(q)$ in exactly q^{K-1} positions.

Proof: Let $\vec{u} = [u_1, \cdots u_K]$ be any non-zero information vector and suppose that $u_k \neq 0$. Then

$$x_i = g_{ki}\, u_k + \sum_{\substack{j=1 \\ j \neq k}}^{K} g_{ji}\, u_j$$

Keep $\vec{u}$ fixed but vary i. Since all nonzero $q^K - 1$, K vectors for $(g_{1i}, \cdots g_{Ki})$ occur, all q^{K-1} possibilities for $(g_{1i}, g_{2i} \cdots g_{k-1,i}, g_{k+1,i} \cdots g_{K,i})$ occur. For any non zero $\alpha \in GF(q)$, there is only one choice for $g_{k,i}$ to make $x_i = \alpha$ for each ~~the~~ of q^{K-1} choices of other g's. Therefore α occurs exactly q^{K-1} times in each code word.

Note: Reason for requiring $\alpha \neq 0$

$g_{ki} = \left(\alpha - \sum_{\substack{j=1 \\ j \neq k}}^{K} g_{ji}\, u_j\right) u_k^{-1}$

$(g_{1i} \cdots g_{k-1,i}, g_{k+1,i}, \cdots g_{K,i}) = \vec{0}$ can occur. Then

$\alpha = 0 \Rightarrow g_{ki} = 0$ and ith column of G is zero which is not allowed.

so $w(\vec{x}) = (q-1)\, q^{k-1}$

From p. 22 $\quad d_{avg} = (q^k - 1)\, q^{k-1} \dfrac{(q-1)}{q^k - 1} = (q-1)\, q^{k-1}$

$= d_{min}$

$R = \dfrac{m}{q^m - 1} \xrightarrow{m} 0$ so not meet ~~to~~ Shannon Bound

Def: Dual Codes

Two linear codes are <u>duals</u> if the generator matrix for one is the parity check matrix for the other

Ex. Let $q = 2$, then the G for maximal length codes is H for Hamming single error correcting code.

5. Golay (23, 12) Code

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$$

$\Rightarrow$ 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

~~A. Varshamov, Gilbert, ABRadel and Hamming Bound~~