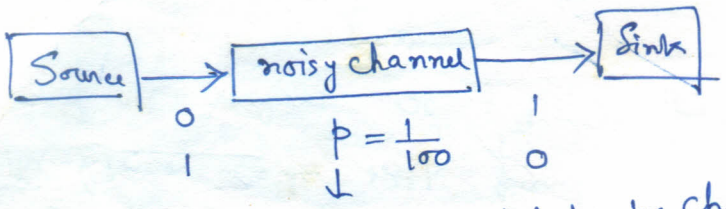
Error correcting codes :



Why?
to give messages some protection against errors on the channel.

Communication channel

- message $u = u_1 u_2 \cdots u_k$ (a block of k symbol) $u_i = 0$ or 1
- codeword $x = x_1 x_2 \cdots x_n$ $x_i = 0$ or 1. $n \geq k$.
- Code → Set of all codewords.

Linear Code $(Hx^T = 0)$

$x_1 = u_1, x_2 = u_2, \ldots, x_k = u_k$ — k message symbols.

$x_{k+1}, x_{k+2}, \ldots, x_n$ — n−k check symbols.

↓ chosen so that

$\boxed{Hx^T = 0}$ property of linear code.

$H_{n-k \times n}$ → parity check matrix of the code.

$H = [A \mid I_{n-k}]$ → standard form.

$A_{n-k \times k}$, I_{n-k} → identity matrix of order n−k.

Example.

$$H = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \quad n-k \times n$$

$$= [A \mid I_3]$$

$n-k = 3$, $n = 6$ $\Rightarrow k = 6-3 = 3$.

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

~~codeword~~

message

u_1	u_2	u_3
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

$C =$

codeword

x_1	x_2	x_3	x_4	x_5	x_6
0	0	0	0	0	0,
0	0	1	1	1	0,
0	1	0	1	0	1,
0	1	1	0	1	1,
1	0	0	0	1	1,
1	0	1	1	0	1,
1	1	0	1	1	0,
1	1	1	0	0	0,

$$Hx^T = 0$$

$$\left[\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = 0 \Rightarrow \begin{cases} x_2 + x_3 + x_4 = 0 \\ x_1 + x_3 + x_5 = 0 \\ x_1 + x_2 + x_6 = 0. \end{cases}$$

parity check equations.

~~linear code~~ Defⁿ: Let H be any binary matrix. The linear code with parity check matrix H consists of all vectors x s.t. $Hx^T = 0$.

Example:

$$H = \begin{bmatrix} 1 & 1 & & & \\ 1 & \cdot & 1 & & \\ 1 & \cdot & \cdot & 1 & \\ 1 & \cdot & \cdot & \cdot & 1 \end{bmatrix} = [A \mid I_4]$$

$Hx^T = 0$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = 0$$

$n-k = 4$, $n = 5$

$\Rightarrow k = 1$.

$\Leftrightarrow$ $x_1 + x_2 = 0$
$x_1 + x_3 = 0$
$x_1 + x_4 = 0$
$x_1 + x_5 = 0$.

message
$u = u_1$
0
1

codeword
$x = x_1 x_2 x_3 x_4 x_5$

$C = \{00000, 11111\}$.

↓

Repetition code.

message symbol is simply repeated 5 times.

Generator matrix

$H_{n-k \times n}$ → parity check matrix, $Hx^T = 0$ gives parity check eqns.

$= [A_{n-k \times k} \mid I_{n-k}]$.

$G_{k \times n}$ → generator matrix of the code.

$u = u_1 u_2 \cdots u_k$.

$x = x_1 x_2 \cdots x_n$

$= x_1 x_2 \cdots x_k x_{k+1} \cdots x_n$.

$x_1 = u_1, x_2 = u_2, \ldots, x_k = u_k$

$$\therefore \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = I_k \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}$$

$Hx^T = 0$ where $H = [A \mid I_{n-k}]$

$$\therefore [A \mid I_{n-k}] \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ x_k \\ x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = 0 \Rightarrow \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = -A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix}$$

$$= -A \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}$$

$$\therefore \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} I_k \\ \hline -A \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}$$

i.e. $x = uG$

where $G_{k \times n} = [I_k \mid -A^T]$.

WEB.

- $Hx^T = 0$
- $H = [A \mid I_{n-k}]$ standard form. parity check matrix $\downarrow$ $n-k \times n$.
- $G = [I_k \mid -A^T]$ generator matrix $\downarrow$ $k \times n$.

- $HG^T = 0$ or $GH^T = 0$.
- $n \rightarrow$ length of the code
- $k \rightarrow$ dimension of the code $\Big\}$ $[n, k]$ code.
- # of codewords $\rightarrow 2^k$.
- rate $\rightarrow \frac{k}{n}$ or efficiency.
- Linearity $\rightarrow$ Vector space over the field, also additive group.

Example: $H = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$ $n = 6, n-k = 3$, $k = 3$

A $\quad$ I_{n-k}

$G = [I_k \mid -A^T]$

$= \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$

$x = uG = (u_1 u_2 u_3) G = u_1 \text{ row}_1 + u_2 \text{ row}_2 + u_3 \text{ row}_3$.

$u_i = 0$ or 1

$\downarrow$ codeword

$\downarrow$ linear combination of rows of G.

$\downarrow$ G generates the code

$u = u_1 u_2 u_3$	$x = x_1 x_2 x_3 x_4 x_5 x_6$
0 0 0	0 0 0 0 0 0
0 0 1	0 0 1 1 1 0
0 1 0	0 1 0 1 0 1
0 1 1	0 1 1 0 1 1
1 0 0	1 0 0 0 1 1
1 0 1	1 0 1 1 0 1
1 1 0	1 1 0 1 1 0
1 1 1	1 1 1 0 0 0

$= C$.

other generator & parity check matrix

- any maximal set of linearly independent codewords can be used as the rows of a generator matrix

$G_{k \times n}$

- **parity check of a code:**

any row vector h s.t. $hx^T = 0$ $\forall$ $x \in \mathcal{C}$.

h: $1 \times n$, x^T: $n \times 1$, x: codeword, $\mathcal{C}$: code

- any maximal set of linearly independent parity checks can be used as rows of a parity check matrix.

Example: $[n, 1]$ Repetition code — H? G?

$H_{n-k \times n}$

- **linearity:**

$H(x+y)^T = Hx^T + Hy^T$

Example. $[n, n-1]$ even wt. code

$H = [1 \; 1 \cdots 1 \; | \; 1]_{n-k \times n}$ $= A | I_{n-k}$ (n terms)

$G = [I_k | -A^T] = [1 \; 0 \cdots 0 \; | \; 1 ; \; 0 \; 1 \cdots 0 \; | \; 1 ; \; \cdots ; \; 0 \; 0 \cdots 1 \; | \; 1]$ ($k \times n$, $n-k \times 1$)

$\Rightarrow ax + by \in \mathcal{C}$, $a, b \in F$.

Example (codes over other fields)

$[4,2]$ ternary code, $H = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{array}\right] = [A | I_{n-k}]$ ← standard form

$n = 4$, $k = 2$ $\quad |\mathcal{C}| = 3^k = 3^2 = 9$.

Find $G \Rightarrow$ generator matrix

Find $\mathcal{C} \rightarrow$ the code i.e. the set of all codewords.

$G = [I_k | -A^T] = \left[\begin{array}{cc|cc} 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -2 \end{array}\right] = \left[\begin{array}{cc|cc} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{array}\right]$

$x = uG = u_1 \text{ row}_1 + u_2 \text{ row}_2$

message $u = u_1 u_2$	codeword $x = x_1 x_2 x_3 x_4$
0 0	0 0 0 0
0 1	0 1 2 1
0 2	0 2 1 2
1 0	1 0 2 2
1 1	1 2 0 1
1 2	2 0 1 1
2 0	2 1 0 2
2 1	2 2 2 0

$1 \; 0 \; -1 \; -1$
$0 \; 2 \; -2 \; -4$

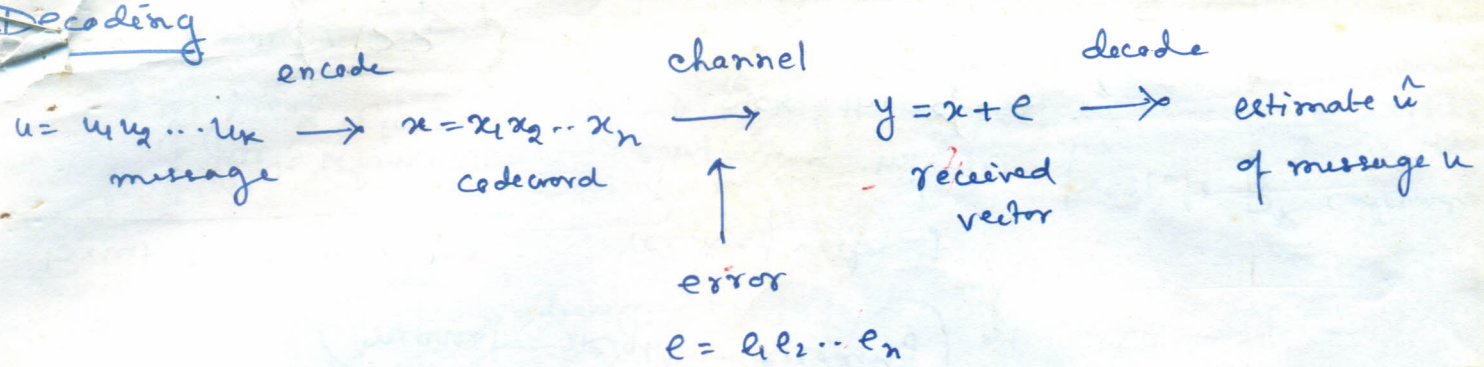
message $u = u_1 u_2$: $0 \; 0$, $0 \; 1$, $0 \; 2$, $1 \; 0$, $1 \; 1$, $1 \; 2$, $2 \; 0$, $2 \; 1$, $2 \; 2$

$-1 \; -2$
$-1 \; -4$

$\omega \neq 0$

$\omega \in \mathcal{C}$.

Decoding



- Decoder can never be certain what e was
- Decoder's strategy → choose most likely error, given that y is received.

(maximum likelihood decoding).

Hamming distance of two vectors $x = x_1x_2 \dots x_n$ & $y = y_1y_2 \dots y_n$

↓

dist(x,y) = # of places where they differ

$x = 10111$
$y = 00102$
dist(x,y) = 2

$x = 0122$
$y = 1220$
dist(x,y) = 3

Hamming weight of a vector $x = x_1x_2 \dots x_n$

↓

wt(x) = # of non-zero x_i in x

wt(10110) = 4, wt(01212110) = 6

- dist(x,y) = wt(x-y).

↓ both

# of places where x, y differ.

an both parts) Check matrices of some Hamming code.

The minimum distance of a code

$d = \min dist(u,v)$

$= \min wt(u-v), \quad u \in C, v \in C, u \neq v.$

$= \min wt(w)$ as for a linear code $u-v$ is a codeword.

$w \in C$

$w \neq 0$

- $[n,k]$ linear code with minimum distance $d \rightarrow [n,k,d]$ code.

- $p \rightarrow$ error probability in a single bit position

$Prob(e=00000) = (1-p)^5$

$Prob(e=01000) = p(1-p)^4$

$Prob(e=10010) = p^2(1-p)^3$

$Prob(e=v) = p^a (1-p)^{n-a}.$

$e \rightarrow$ error vector of length n

$v \rightarrow$ a vector with wt. a

Maximum likelihood decoding

↓

most likely error vector e is chosen by the decoder.

↓

nearest neighbor decoding

- $p < \frac{1}{2}$ $\quad (1-p)^5 > p(1-p)^4 > p^2(1-p)^3 > \cdots$

e with wt. 1 is more likely that e with wt. 2, & so on.

Decode's strategy: Pick the error vector e which has least wt.

(nearest neighbor decoding).

Brute force decoding.

↓ fails when k is large

received vector y

↓

compare y with all possible 2^k codewords & pick the closest.

Method ??

Theorem: a code with minimum distance d can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

- if d is even, the code can simultaneously correct $\frac{d-2}{2}$ errors & detect $\frac{d}{2}$ errors.

proof:

Sphere of radius r, centre at u

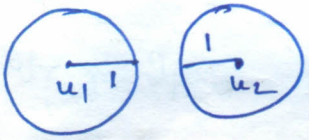
$$\rightarrow S_u(r) = \{ v \mid \text{dist}(u,v) \leq r \}$$

$S_r(u)$

$d=3$ $r=1$ draw a sphere of radius 1 around each codeword.

↓

these spheres do not overlap as min. dist. of the code is 3.



- $u \xrightarrow{\text{transmitted}}$ a received vector $\Rightarrow$ received vector a is inside the sphere around the codeword u.
- 1 error occur

$\text{dist}(u,a) \leq 1$.

$\Rightarrow a \in S_u(1)$.

↓

nearest neighbor decoding corrects this error.

a closer to u than any other codeword v

$d = 2t+1$ $r = t$

$u \rightarrow a$

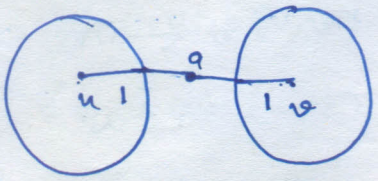
$\text{dist}(u,a) \leq t$.

non-overlapping spheres of radius t around each codeword.

↓

nearest neighbor decoding corrects t errors.

d even d=4



u, v codewords

1 errors → dist(a,u) = 1 → a is corrected by u. detect correct $\frac{d-2}{2}$ error

2 errors → dist(a,u) = 2 → a may be midway between u, v.

→ can detect 2 errors, but cannot correct it. $= \frac{d}{2}$

Decoding of a linear code

- $\mathcal{C} \to [n,k]$ linear code over F_q.
- $a \to$ any vector of length n
- $a + \mathcal{C} = \{a+x : x \in \mathcal{C}\} \to$ a coset of $\mathcal{C}$.

↓

q^k vectors

- each vector b of length n is in some coset. ($b \in b + \mathcal{C}$).
- a, b are in the same coset of $\mathcal{C}$ iff $a - b \in \mathcal{C}$.
- Two cosets → $a+\mathcal{C}$, $b+\mathcal{C}$ → either disjoint or coincide (partial overlap is impossible).

Let $a+\mathcal{C}$, $b+\mathcal{C}$ overlap

Let $v \in (a+\mathcal{C}) \cap (b+\mathcal{C})$

$\therefore v = a + x = b + y$, $x, y \in \mathcal{C}$.

↓

$x - y \in \mathcal{C}$

$\Rightarrow b = a + (x-y) \in a + \mathcal{C}$.

Then $b \in b + \mathcal{C} \Rightarrow b \in a + \mathcal{C}$

$\therefore b + \mathcal{C} \subseteq a + \mathcal{C}$.

Similarly,

$a + \mathcal{C} \subseteq b + \mathcal{C}$

$\therefore a + \mathcal{C} = b + \mathcal{C}$.

- $F^n \rightarrow$ partitioned into disjoint cosets
  $\rightarrow$ each coset having q^k elements.

$$F^n = \mathcal{C} \cup (a_1 + \mathcal{C}) \cup (a_2 + \mathcal{C}) \cup \cdots (a_t + \mathcal{C})$$

(F^n: q^n; $\mathcal{C}$: q^k; $(a_1+\mathcal{C})$: q^k; $(a_2+\mathcal{C})$: q^k; $(a_t+\mathcal{C})$: q^k.)

where

$$q^n = (q^k + q^k + \cdots + q^k) \quad (t+1 \text{ terms})$$

$$= (t+1) q^k$$

$$\therefore t = q^{n-k} - 1.$$

- y received vector

$\therefore$ y is in some coset, say $y \in a + \mathcal{C}$.

$\therefore y = a + x, x \in \mathcal{C}$.

Let codeword x' was transmitted

Then error $e = y - x' = a + \underbrace{x - x'}_{\in \mathcal{C}}, \; x, x' \in \mathcal{C}$

$\in a + \mathcal{C}$

Thus $y, e \in a + \mathcal{C}$.

i.e. error vector $\in$ the coset containing y

are both parity check matrices of same [illegible]

• possible error vectors are exactly the vectors in the coset containing y.

• nearest neighbor decoding → error vector with least weight.

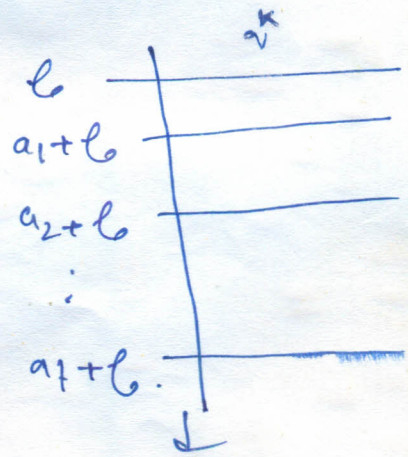
• Decoder's strategy → pick the minimum wt. vector $\hat{e}$ (coset leader) in the coset containing y & decode y as $\hat{x} = y - \hat{e}$.

Standard array

Example: $G = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right)_{2\times 4}$ $\quad I \mid -A^T$

$H = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right)$ $\quad n-k \times n$, 2×4

$t = 2^{4-2} - 1 = 4 - 1 = 3.$



$t = q^{n-k} - 1$

message: $u = u_1 u_2$

message:	00	10	01	11	Syndrome
code :	0000	1011	0101	1110	$\begin{pmatrix}0\\0\end{pmatrix}$
coset :	1000	0011	1101	0110	$\begin{pmatrix}1\\1\end{pmatrix}$
coset :	0100	1111	0001	1010	$\begin{pmatrix}0\\1\end{pmatrix}$
coset :	0010	1001	0111	1100	$\begin{pmatrix}1\\0\end{pmatrix}$

skip for syndrome decoding.

received vector $y = 1111$

$e = 0100$

$\hat{x} = 1011$

or

$\hat{u} = 10$

Syndrome

$[n, k]$ linear code with parity check matrix H

let $y \rightarrow$ received vector

Syndrom of $y \rightarrow Hy^T$.

$$y = x + e \quad , x \in C$$

$$Hy^T = He^T .$$

if $e = 0 \cdots 0 \,|\, 0 \cdots 1 \cdots 1 \cdots 0$,
(a | b | c)

$$S = Ha + Hb + Hc + \cdots$$

($Hi \rightarrow i$th colum of H)

- Two vectors are in the same coset of C iff they have the same syndrome.

$u, v \rightarrow$ two vectors $\in a + C$.

$\therefore$ iff $u - v \in C$.

$\therefore H(u-v)^T = 0$

$Hu^T = Hv^T$

Thus vectors u, v have the same syndrom.

- 1-1 correspondence between syndromes & cosets.

Syndrome decoding

$y = 111 \,|$

$$Hy^T = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right)\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$\hat{u} = 10 \Leftarrow \hat{x} = y - e = 1011 \Leftarrow e = 0100$

Example :2 Binary Repetition Code with $n=4$.

$q=2, \quad k=1$

$$F_2^4 = C \cup (a_1+C) \cup (a_2+C) \cup \cdots \cup (a_t+C)$$

with $t = q^{n-k} - 1$

$= 2^3 - 1 = 7$

$|F_2^4| = 2^4$.

$d = 4$

⇓

1 error correcting & 2 error detecting

Standard Array

m :	0	1	S
c :	0000	1111	(0 0 0)
coset :	1000	0111	(1 1 1)
	0100	1011	(1 0 0)
←	0010	1101	(0 1 0) →
	0001	1110	(0 0 1)
	1100	0011	(0 1 1)
	1010	0101	(1 0 1)
	1001	0110	(1 1 0)
	coset leaders		

$^4C_2 = \frac{4!}{2!2!} = 6$.

Received vector : $y = 1011$

$\therefore \hat{e} = 0100$ — coset leader

$\therefore \hat{x} = 1111$

$\hat{e} = 1$

$\therefore \hat{w} = 1$

Perr = ?

$\alpha_0 = 1, \alpha_1 = 4, \alpha_2 = 3$

$P_{err} = 1 - (1-p)^4 - 4p(1-p)^3 - 3p^2(1-p)^2$

$= ?$ if $p = \frac{1}{100}$

- Any choice of std-array → can correct 3 error pattern of wt. 2.

~~Received vector~~

- This choice of array corrects all error-pattern of wt. 0, 1, but only error pattern of wt. 1100, 1010, 1001 of wt. 2 & none of wt. 3 or 4.

$H = \underset{n-k \times n}{\underset{3\times 4}{}} \left[\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array}\right]$

$G = \underset{k\times n}{\underset{1\times 4}{}} \left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \end{array}\right]$

$I_k \mid -A^T$.

$H = \underset{n-k \times n}{\underset{3\times 4}{}} \left[\begin{array}{c|ccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right]$

$A \mid I_{n-k}$.

Example: $\alpha_0 = 1$, $\alpha_1 = 3$

$P_{err} = 1 - (1-p)^4 - 3p(1-p)^3$

$= .0103$ if $p = \frac{1}{100}$

Received vector: $y = 1101$

$S = Hy^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \rightarrow \hat{e} = 0010$.

$\hat{x} = y - \hat{e} = 1101 - 0010 = 1111$

$\hat{u} = 1$.

Error Probability

$\mathcal{C}: x_1, x_2, \ldots, x_M$

$\rightarrow M$ codewords

$P_{err} = Prob\{e \neq \text{coset leader}\}$ — **Std. Arrays.**

↓ decoder outputs wrong codeword.

- $\alpha_i \rightarrow$ # of coset leaders having wt. i

$\therefore P_{err} = 1 - \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}$

$p \rightarrow$ error probabilities in a single position → channel error probability

- Std. Arrays does maximum likelihood decoding

So for other decoding schemes $P_{err} \geq 1 - \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}$

let $d = 2t+1$ → t error correcting code

∴ every vector of wt $\le t$ is a coset leader

$$\therefore \alpha_i = \binom{n}{i}, \quad 0 \le i \le t.$$

for $i > t$, α_i calculations are extremely difficult.

Approximation

Channel error probability p → small.

$$\therefore 1-p \approx 1.$$

$$\text{if } p^i(1-p)^{n-i} \gg p^{i+1}(1-p)^{n-i-1}$$

neglecting terms with large i

$$P_{err} \approx 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}$$

$\le$

or

$$P_{err} \approx 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i} - \alpha_{i+1} p^{i+1} (1-p)^{n-i-1}$$

$\le$

equality → perfect t error correcting code. → can correct all errors of wt. $\le t$ & none of wt. $> t$.

i.e. $\alpha_i = 0 \quad \forall\, i > t = \left\lfloor \frac{d-1}{2} \right\rfloor$

↓

spheres of radius t around the codewords are disjoint & together contains all vectors of length n

equality → quasi perfect t-error correcting code.

i.e. $\alpha_i = 0 \quad \forall\, i > t+1.$

↓

can correct all errors of wt. $\le t$, some of wt. $t+1$, & none of wt. $> t+1$

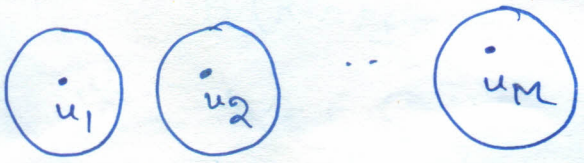
↓

Sphere of radius $t+1$ around each codewords may overlap & together contains all vector of length n.

- **Perfect code** → t-error correcting perfect code

$\mathcal{C} \to [n, k]$ linear code over F_q

- q^n vectors total of length n
  ↓
  $M = q^k$ are codewords.
  ↓
  sphere around codewords of radius t non-overlapping & together contains all q^n vectors of length n.



$S_t(u_i)$ • $S_{u_i}(t) = \{ v \mid \text{dist}(u_i, v) \le t \}$,

$S_{u_i}(t) \cap S_{u_j}(t) \neq 0$, $u_i, u_j \in \mathcal{C}$.

$$\left| \bigcup_{i=1}^{M} S_{u_i}(t) \right| = q^n.$$

t-error correcting

- **Quasi-Perfect code** → the spheres of radius $t+1$ around each codeword may overlap & together contains all the q^n vectors of length n.

Sphere Packing / Hamming Bound

$\mathcal{C} \to [n, k]$ linear code, t-error correcting, binary (say).

$M = 2^k$ codewords
↓
draw a sphere of radius t around each codeword

$$|S_{u_i}(t)| = |\{ v \mid \text{dist}(u_i, v) \le t \}|$$
$$= \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}$$

M such spheres ∴ $M\left[\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}\right] \le 2^n$.

↓ equality when $\mathcal{C}$ is pe

Hamming code → Perfect, single error correcting code.

Why?

↓

* H_r of length $n = 2^r - 1$ has parity check matrix whose columns are all non-zero binary vectors of length r.

↓

$$\left[n = 2^r - 1,\ k = n - r = 2^r - 1 - 1,\ d = 3 \right] \text{ code.}$$

$n = 2^r - 1 \Rightarrow n + 1 = 2^r$

$k = n - r \Rightarrow k + r = n$

$d = 3$ — Why?

~~• if $d = 3$ then single-error correcting as $\left[\frac{d-1}{2}\right] = 1$.~~

• Perfect.

$$M \left[\binom{n}{0} + \binom{n}{1} \right] = 2^k \cdot [1 + n]$$

$M = 2^k$

$$= 2^k \cdot 2^r = 2^{k+r} = 2^n.$$

equality holds in Hamming sphere packing bound.

• Single error correcting

Parity check matrix

$H = (H_1, H_2, \cdots, H_n)$ — $r \times n$

↓ binary representation of i (r-tuple).

$r \rightarrow$ # of parity checks.

• $d = 3$ Since single-error correcting, $d \geq 3$.

$11100\cdots0$ is a codeword $\Rightarrow d = 3$ of wt. 3.

Syndrome decoding

If y is received.

$$Hy^T = He^T.$$

$= H_i$ (if error occur at i-th position)

= binary representation of i.

$e = 00\cdots\underset{\text{a-th position}}{1}0\cdots0\underset{\text{b-th position}}{1}00\cdots\underset{\text{c-th position}}{1}0\cdots$

$y = x + e$

$Hy^T = He^T = H_a + H_b + H_c + \cdots$

Single error means one column of H.

are both parity check matrices of same linear code.

$$\therefore M\left[\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right] \le 2^n$$

↓ over binary field F_2

Over other field, say F_q (q finite).

$$M\left[\binom{n}{0}+(q-1)\binom{n}{1}+(q-1)^2\binom{n}{2}+\cdots+(q-1)^t\binom{n}{t}\right] \le q^n$$

Perfect code if equality holds.

Example: (Hamming code)

Shannon's Main Theorem.

on existence of good codes. (without proof).

for binary symm. channel.

for any $\varepsilon > 0$, if $R < C(P) = 1 - H_2(P) = 1 - P\log_2\frac{1}{P} - \bar{P}\log_2\frac{1}{\bar{P}}$

& n is sufficiently large, there is an $[n, k]$ binary code of rate $\frac{k}{n} \ge R$ with error probability $P_{err} < \varepsilon$.

Then $P_{err} = \frac{1}{M}\sum_{i=1}^{M} \text{Prob}\{\text{decoder output} \neq x^{(i)} \mid x^{(i)} \text{ was sent}\}$

$\mathcal{C} = \{x^{(1)}, \ldots, x^{(M)}\}$ being the codewords of the

Equivalent codes:

C_1, C_2 equivalent if they differ only in the order of the symbols

$$C_1 = \{0000, 0011, 1100, 1111\}, \quad C_2 = \{0000, 0101, 1010, 1111\}.$$

$C_1, C_2 \rightarrow$ equivalent

generator matrix

elementary row operations + column permutation.

$G_1 \longrightarrow G_2$.

G_1, G_2 generate equivalent codes.

Example: Hamming code $[7, 4, 3]$

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

$$H' = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \rightarrow \text{standard form. } [A \mid I_r]$$

...gleton bound $[n,k,d]$ linear code.

$d \le n-k+1$.

$G = [I_k | A]$ $\rightarrow$ each row is a non-zero codeword of weight at most $1+(n-k)$

$A_{k \times n-k}$.

$\therefore$ min. dist.

$d \le 1+(n-k)$.

exactly 1 non-zero information digit

+

$n-k$ check digits in A.

+

min dist. = min. wt. of any codeword.

Gilbert - Varshamov Bound

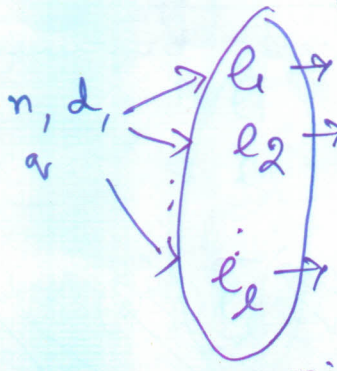
- $[n,k]$ linear code over F_q.

i.e. q^k codewords, each of length n.

size q^n

$q \ge 2, \; n \ge d \ge 1$.

- $A_q(n,d)$ $\rightarrow$ max. no. of codewords in any q-ary code of length n & min. dist. d.



all possible codes. (not necessarily linear)

$A_q(n,d) = \max_i M_i$

Hamming sphere Packing Bound

$A_q(n,d) \left[\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t} \right] \le q^n$

where $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

are both parity check matrices of some linear code.

Gilbert-Varshamov bound

$$A_q(n,d)\left[\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{d-1}\right]\geq q^n$$

Hamming sphere Packing Bound. $q\geq 2,\ n\geq d\geq 1$

$$A_q(n,d)\left[\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right]\leq q^n$$

where $t=\left\lfloor\frac{d-1}{2}\right\rfloor$

Gilbert-Varshamov bound $q\geq 2,\ n\geq d\geq 1$

$$A_q(n,d)\left[\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{d-1}(q-1)^{d-1}\right]\geq q^n$$

for fixed q, n, d, let $\mathcal{C}$ be the code having max^m. # of codewords.

$\therefore M=|\mathcal{C}|=A_q(n,d)$.

for each $u\in\mathcal{C}$

$$S_{d-1}(u)=\left\{v\in F_q^n \;\middle|\; \text{dist}(u,v)\leq d-1\right\}.$$

$$\therefore |S_{d-1}(u)|=\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{d-1}(q-1)^{d-1}.$$

if some $v\in F_q^n$ is not in any $S_{d-1}(u)$, then $\text{dist}(u,v)\geq d-1$ i.e. $\text{dist}(u,v)\geq d$ $\forall u\in\mathcal{C}$.

In this case the code $\mathcal{C}' = \mathcal{C} \cup \{v\}$ has same q, n, d values with $|\mathcal{C}'| > |\mathcal{C}|$ $(\rightarrow\leftarrow)$ as $\mathcal{C}$ was chosen to have max^m. # of codewords $A_q(n,d)$.

$\therefore$ each sphere $S_{d-1}(u)$, $u \in \mathcal{C}$ contains

$$\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{d-1}(q-1)^{d-1}$$

vectors in F_q^n, & all the q^n vectors in F_q^n are contained by these spheres & there are $A_q(n,d)$ such spheres.

$\therefore$ $A_q(n,d)\left[\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{d-1}(q-1)^{d-1}\right] \geq q^n$.

Hamming code $\rightarrow$ H with any 2 cols. lin. ind. & all cols. distinct. $\rightarrow$ min. dist. $= 3$.

↓ a vector of F_q^n may be counted more than once in case spheres overlap.

Theorem $[n,k]$ linear code with parity check matrix H. Then rank of $H = n-k$.

i.e. some $n-k$ colums of H are linearly ind.

(as row rank = col. rank = rank of H).

Theorem $[n,k]$ linear code $\mathcal{C}$ with parity check matrix H.

Min. dist. is d iff every $d-1$ cols. of H are lin. ind. & some d cols. are lin. dep. (as $x \in \mathcal{C}$ with $wt(x) = w$ iff $Hx^T = 0$ iff some w cols. of H are lin. dep.; $w \geq d$, $w \leq d$)

are both parity check matrices of same linear code.

Dual code

- $\mathcal{C} \to [n, k]$ linear code over F_q
- $\mathcal{C}^\perp \to$ dual or orthogonal code of $\mathcal{C}$

$$\mathcal{C}^\perp = \{ u \in F_{q^n} \mid u \cdot v = 0 \ \forall \ v \in \mathcal{C} \}$$

(u, v are orthogonal)

$u = u_1 u_2 \cdots u_n$, $v = v_1 v_2 \cdots v_n$

$u \cdot v = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n$

- $\mathcal{C}^\perp \to$ set of all parity checks on $\mathcal{C}$.

$h \in F_{q^n}$ is a parity check on $\mathcal{C}$ if $hx^T = 0 \ \forall \ x \in \mathcal{C}$.

- $\mathcal{C} \to$ generator matrix $G_{k \times n}$, parity check matrix $H \to [n, k]$ code
- $\mathcal{C}^\perp \to$ generator matrix $H_{n-k \times n}$, parity check matrix $G \to [n, n-k]$ code.
- $\mathcal{C} \subset \mathcal{C}^\perp \to$ $\mathcal{C}$ is weakly self dual $\to u \cdot v = 0 \ \forall u, v \in \mathcal{C}$.
- $\mathcal{C} = \mathcal{C}^\perp \to$ $\mathcal{C}$ is strictly self dual $\to u \cdot v = 0 \ \forall u, v \in \mathcal{C}$ + $k = \frac{1}{2} n$ (i.e., n is even)

Example. Repetition code of length n. ($k = 1$)

Binary

$$\mathcal{C} = \{ \underbrace{00\cdots0}_{u}, \underbrace{11\cdots1}_{v} \}$$

$u \cdot u, u \cdot v, v \cdot u, v \cdot v = 0$ if n is even $\Rightarrow$ $\mathcal{C}$ is weakly self dual iff n is even

$n = 2$ $\mathcal{C} = \{00, 11\}$ $\quad k = 1 = \frac{1}{2} n \Rightarrow \mathcal{C}$ is strictly self dual.

Dual of Hamming code $\to$ Simplex code.

$H_r \ [n = 2^r - 1, k = n - r]$ $\quad$ generator matrix $\quad$ $S_r \ [n = 2^r - 1, n - k = r]$

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Other generator & parity check matrices

- A code can have several different generator matrices

Example: $G_1 = \begin{bmatrix} 1&1&1&0 \\ 0&1&0&1 \end{bmatrix}$, $G_2 = \begin{bmatrix} 1&0&1&1 \\ 0&1&0&1 \end{bmatrix}$

are both generator matrices of a linear code.

- Any maximal set of linearly independent codewords taken from a given code can be used as the rows of a generator matrix for that code.

$G_{k \times n}$ → rank k.

~~G_2 → Std. form.~~

- $C_1 = \{1110, 0101, 1011\}$
- $C_2 = \{1011, 0101, 1110\}$

[exact same code]

equivalent code

↓

$G_1 \rightarrow G_2$ by elementary row operations & column permutation

- Parity check matrix → $Hx^T = 0 \; \forall x \in C$ → H is a parity check

Example: Hamming code with r parity checks (H_r)

- any r lin. ind. parity checks can be taken as row of H_r.

Example: $H_1 = \begin{bmatrix} 1&0&1&0 \\ 1&1&0&1 \end{bmatrix}$, $H_2 = \begin{bmatrix} 0&1&1&1 \\ 1&1&0&1 \end{bmatrix}$

are both parity check matrices of same linear code.

- $H_1 = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right]$ ⇒ (Std. form)

$A \mid I$

$x_1 + x_3 = 0$

$x_1 + x_2 + x_4 = 0$

u_1	u_2
0	0
0	1
1	0
1	1

x_1	x_2	x_3	x_4
0	0	0	0,
0	1	0	1,
1	0	1	1,
1	1	1	0, }

C_1

- $H_2 = \left[\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{array}\right] \rightarrow H_3 = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right]$ ⇒ (Std form)

interchange x_1 & x_4

$x_1 + x_2 + x_3 = 0$

$x_1 + x_2 + x_4 = 0$

u_1	u_2
0	0
0	1
1	0
1	1

x_4	x_2	x_3	x_1
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

C_2

interchange x_1 & x_4 of C_1

{ 0 0 0 0,
1 1 1 0,
1 0 1 1,
0 1 0 1, }

C_1, C_2 are exactly same

A

- Parity check on a code $\mathcal{C}$ is any row vector h s.t. $hx^T = 0$ $\forall x \in \mathcal{C}$.

- Any maximal set of linearly independent parity checks can be used as the rows of a parity check matrix H for $\mathcal{C}$.

- $H_{r \times n}$ → rank r.

  → parity check matrix of a code of length n with dimension $k = n - r$.

  → r columns of H are linearly independent, but no $r+1$ columns are.

Theorem

linear code

* $\mathcal{C}$ with parity check matrix $H_{r \times n}$ with minimum distance d iff every $d-1$ columns of H are linearly independent & some d columns are linearly dependent.

proof.

$x \in \mathcal{C}$ with $wt(x) = w$

iff

$Hx^T = 0$ with $wt(x) = w$

iff

some w columns of H are linearly dependent.

mindist $\Rightarrow d \Rightarrow \exists$ some $x \in \mathcal{C}$ with $wt(x) = d$, $x \neq 0$.

$\Rightarrow$ some d columns of H are lin. dep.

Since d is min $\Rightarrow$ no $d-1$ columns of H are lin. dep.

$\Rightarrow$ no $x \in \mathcal{C}$ with $wt(x) < d$.

• Hamming code has min. dist. $d = 3$.

H_r → parity check matrix

→ columns of all non-zero r-tuples.

$n = 2^r - 1$ such columns.

→ all distinct. If so any two column are lin. independent, and there are 3 columns which are lin. dependent.

⇒ min. dist. $d = 3$.

• Singleton bound. If C is an $[n, k, d]$ code, then $n - k \geq d - 1$.

proof. ⊕ parity check matrix $H_{n-k \times n}$ has rank $r = n - k$ ⇒ r is the max^m no. of lin. ind. columns.

d min dist. of C ⇒ every $d-1$ columns of H are lin. ind.

$\therefore$ $n - k \geq d - 1$.

Alternative proof.

$G_{k \times n} = [I_k \mid A_{k \times n-k}]$ → each row in a non-zero codeword of wt. at most $1 + (n-k)$.

d is min dist. i.e. min. wt. of a non-zero codeword

$\therefore d \leq 1 + (n-k)$

• Equality holds i.e. $r = d - 1$ → MDS code (Connected to finite geometry)

(Maximum distance separable)

Upper bound on size of a code; given $q, n, d \to k$ or q^k or $A_q(n,d)$

- **Hamming-Sphere-Packing Bound.** $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

~~$A_q(n,d)\left[\binom{n}{0}+\binom{n}{1}+\cdots\right]$~~

$$A_q(n,d)\left[\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right] \le q^r$$

- **Singleton bound**

$$n-k \geq d-1$$

i.e. $d \le n-k+1$ or $k \le n-d+1$.

Lower bound on size of a code, given $q, n, d \to k$ or q^k or $A_q(n,d)$

- **Gilbert-Varshamov bound.**

$$A_q(n,d)\left[\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{d-1}(q-1)^{d-1}\right] \geq q^n.$$

- **An improvement in the prime power case.**

for q a prime power, one can improve the bound to $A_q(n,d) \geq q^k$ where k is the greatest integer for which

$$q^k < \frac{q^n}{\sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i}$$

value of d s.t. # of codewords of wt $< d$ ~ # of possible syndromes.

i.e. $1+\binom{n-1}{1}+\binom{n-1}{2}+\cdots+\binom{n-1}{d-2} < q^{n-k} = q^r$. on av., any syndrome

- Sphere packing bound, Singleton bound → upper bound on the size of a code with minimum distance.

given q, n, d → k?? or $M = q^k$?? → $A_q(n,d)$.

$[n, k, d]$ → (n, M, d). equivalently.

$$A_q(n,d) \leq \frac{q^n}{X}$$

- The Gilbert-Varshamov bound → lower bound on the size of the code.

→ $A_q(n,d)$

$$A_q(n,d) \geq \frac{q^n}{Y}$$

(Improvement in Gilbert-Varshamov bound).

Example: Prove that there exists a binary linear code of length n, with at most r-parity checks and minimum distance at least d, provided

$$1 + \binom{n-1}{1} + \binom{n-1}{2} + \cdots + \binom{n-1}{d-2} < 2^r = 2^{n-k}.$$

$\Rightarrow 2^k < \frac{2^n}{Z}$ and $A_q(n,d) > q^k$, k being the greatest such integer.

Soln: Construct $r \times n$ matrix H with the property that

→ (P) every $d-1$ columns are lin. indep.

$H = [H_1 \; H_2 \; \cdots \; H_n]$, $H_{r \times n}$

Choose any non-zero r-tuple.

from remaining $n-1$ columns, choose column, such that it is not a lin. combination of $d-2$ or fewer columns with property (P). # of lin. combination of $d-2$ or fewer columns with property (P) $= \binom{n-1}{1} + \cdots + \binom{n-1}{d-2}$

every column H_i of H is a non-zero r-tuple

$\binom{n-1}{1} + \cdots + \binom{n-1}{d-2} < 2^r - 1$

~~if $\binom{n-1}{1} + \binom{n-1}{2} + \cdots + \binom{n-1}{d-2} > 2^r - 1$.~~

Proof. We shall construct an $r \times n$ matrix H with the property that

(P) No $d-1$ columns are linearly dependent. ↓ even $d-1$ colm lin. ind.

as follows:

- We are given r & d.
- The first row H_1 of H can be any ~~r-tuple~~ non-zero r-tuple.

$$H = \begin{matrix} 1 \\ 2 \\ \vdots \\ r \end{matrix} \overbrace{\begin{pmatrix} H_1 & H_2 & \cdots & H_n \end{pmatrix}}^{i \text{ columns}}$$

- Now suppose we have chosen $i \to r^{d-1}$ columns ~~So H~~ with property P.
- Then are $\binom{i}{1} + \binom{i}{2} + \cdots + \binom{i}{d-2}$ distinct linear combinations of these i columns ~~with~~ taken $d-2$ or fewer at a time.
- Provided this number is $< 2^r - 1$, we can add another column different from these linear combinations, and keep the property P in the new $r \times (i+1)$ array.
- We keep on doing this as long as

$$\binom{i}{1} + \binom{i}{2} + \cdots + \binom{i}{d-2} < 2^r - 1.$$

- final i ~~is~~ i.e. i for which no more column can be added, given the value of $n-1$.

Hence $\binom{n-1}{1} + \binom{n-1}{2} + \cdots + \binom{n-1}{d-2} < 2^r - 1$.

Unicity of syndrome preimage

H, $x \in \mathcal{C}$, $wt(x) = w$.

$s = Hx^T$.

prob. on the random choice of H, x

that $\exists\ y \neq x$, $wt(y) = w$ s.t.

$$Hy^T = s. \leq \frac{\sum_{i=0}^{2w} \binom{n}{i}}{2^n}.$$

proof -

$$Hy^T = s = Hx^T$$

$$\Rightarrow H(x-y)^T = 0$$

$$\Rightarrow x - y \in \mathcal{C}$$

$wt(x-y) \leq 2w$.

$$\therefore \sum_{i=0}^{2w} \binom{n}{i} = \#\text{ of codewords of wt } 2w$$

$$\leq 2^{n-k}.$$

$\downarrow$

# of possible syndromes.

Note $\sum_{i=0}^{2w} \binom{n}{i} \sim \binom{n}{2w}$.

$\frac{\binom{n}{2w}}{2^n} < 2^{-80}$ → assures with very good prob. the uniqueness of a preimage of any syndrome

unicity is assured for a very good prob. when $2w$ is little below the GV bound for a random code.

Construction of new codes from old

- Extending a code by adding an overall parity check.

$\mathcal{C} \to [n, k, d]$ with some codewords having odd weight.

$\downarrow H$

if odd. $u = u_1 u_2 \cdots u_n$

then $\downarrow$

$\hat{\mathcal{C}} \to [n+1, k, d+1]$ $\quad u_1 u_2 \cdots u_n \underline{u_{n+1}}$

$\to 0$ if $wt(u) =$ even

$\to 1$ if $wt(u) =$ odd.

even wt. code

$\downarrow$

$\hat{H}$ new parity check equation $\to u_1 + u_2 + \cdots + u_{n+1} = 0$.

$$\hat{H}_{n-k+1 \times n+1} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & & & 0 \\ \vdots & & H & \vdots \\ 0 & & & 0 \end{bmatrix}_{n-k \times n}$$

$\to u_1 u_2 + \cdots + u_{n+1} =$ even

Example: Extended Hamming code $\mathcal{H}_3$

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

location 1 2 3 4 5 6 7 0

$\mathcal{H}_3 \to [7, 4, 3]$

$\hat{\mathcal{H}}_3$ $[8, 4, 4] \to$ can correct 1 error & detect 2 errors.

Syndrome decoding for $\hat{\mathcal{H}}_3$

$S = \hat{H} y^T$

compute syndrome of the received vector y

~~if $S = 0$, no error~~

if no error, $S = 0$

if 1 error at location i, then $S = \begin{pmatrix} 1 \\ x \\ y \\ z \end{pmatrix}$

where $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ is the binary representation of i.

if 2 errors at location i, j, then $S = \begin{pmatrix} 0 \\ x \\ y \\ z \end{pmatrix}$ → seeing this, 2 or even no. of errors found.

→ detects double error, but cannot correct it.

- Puncturing a code by deleting one or more coordinates

→ inverse of ↑ to extending

$\mathcal{C}[n,k,d] \rightarrow \mathcal{C}^*[n-1, k, d-1]$

0 0 0	0 0
0 1 1	0 1
1 0 1	1 0
1 1 0	1 1

↑ delete

$\mathcal{C}[3,2,2] \rightarrow \mathcal{C}^*[2,2,1]$

- Expurgating by throwing away codewords

$\mathcal{C}[n,k,d] \longrightarrow \mathcal{C}'[n, k-1, d']$, $d' \geq d$

even wt + odd wt codewords — throw away all codewords of odd wt.

- Binary linear code → all codewords have even weight

→ or

→ $\frac{1}{2}$ have odd wt., $\frac{1}{2}$ with even wt.

- Augmenting by adding new codewords

provided 1 is not already in $\mathcal{C}$.

$\mathcal{C}[n,k,d]$ $\quad 1+\mathcal{C}$ → complement of $\mathcal{C}$.

$\mathcal{C}^{(a)} = \mathcal{C} \cup \{1+\mathcal{C}\}$. Let d' → largest wt. of a codeword in $\mathcal{C}$.

$[n, k+1, d^{(a)}]$ $\quad d^{(a)} = \min\{d, n-d'\}$

This is equivalent to, adding a row of 1's in the generator matrix of $\mathcal{C}$.

- Lengthening by adding message symbols

augment, then extend. $\mathcal{C}^{(a)}_2 \mathcal{C} \cup$

$\mathcal{C}[n,k,d]$ $\xrightarrow{\text{lengthening}}$ $\{1+\mathcal{C}\}$ $\xrightarrow{\text{add one more parity check bit}}$ to make $\mathcal{C}^{(a)}$ even wt codes

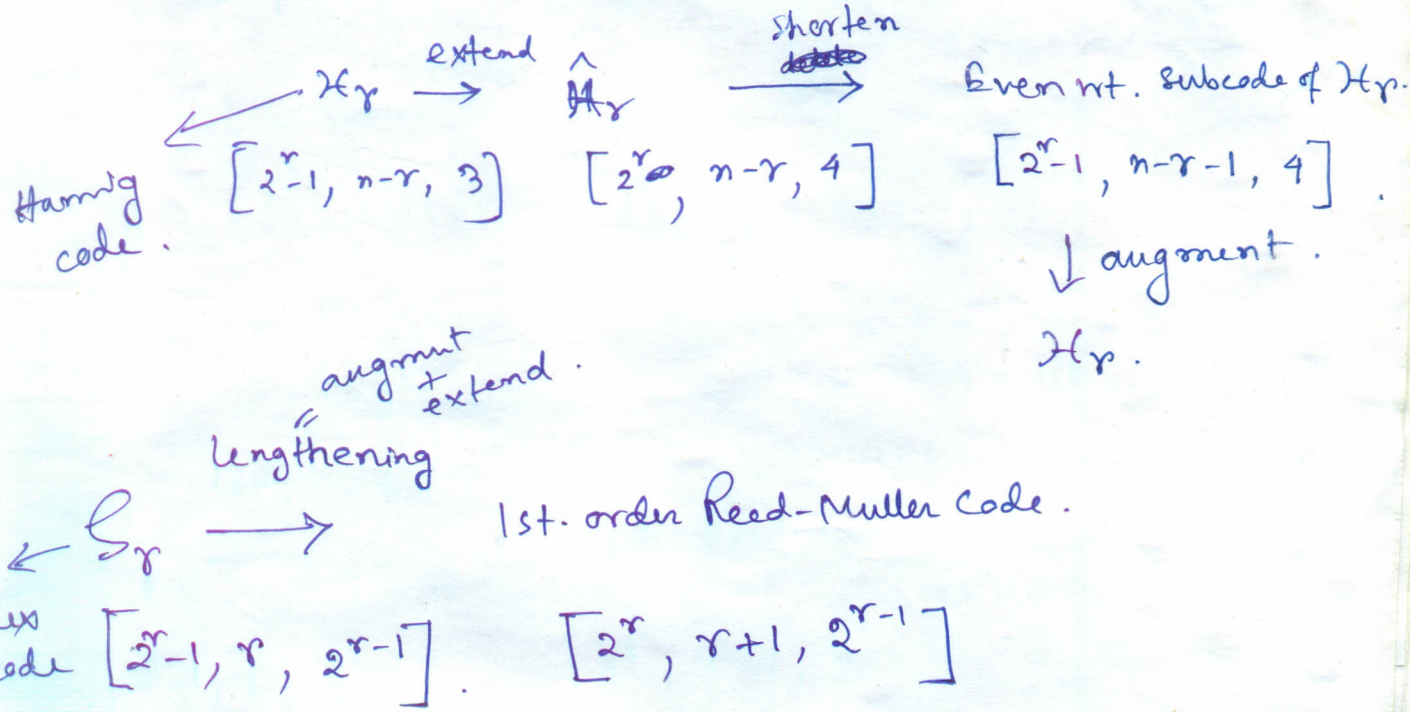
shortening a code by taking a cross section

→ inverse to lengthening process

Choose all the codewords with $x_i = 0$.

& delete the x_i co-ordinate.

- dual of extended Hamming code
  → 1st. order Reed-Muller code.



ruction of new codes from old codes

- $C_1 (n_1, M_1, d_1)$, $C_2 (n_2, M_2, d_2)$

$$C_1 \oplus C_2 = \{ u|v \mid u \in C_1, v \in C_2 \}$$

$(n_1+n_2,\ M_1 M_2,\ d = \min\{d_1, d_2\})$ code.

$z_1 = u_1|v_1 \in C_1 + C_2$ $\quad u_1, u_2 \in C_1$

$z_2 = u_2|v_2 \in C_1 + C_2$. $\quad v_1, v_2 \in C_2$.

$\therefore \text{dist}(z_1, z_2) = \text{dist}(u_1, u_2) + \text{dist}(v_1, v_2)$

$\geq \min\{d_1, d_2\}$.

- $\text{dist}(u_1, u_2) \geq d_1$ if $v_1 = v_2$
- $\text{dist}(v_1, v_2) \geq d_2$ if $u_1 = u_2$.

$$\min \text{dist}(z_1, z_2) = \begin{cases} d_1 & \text{if } v_1 = v_2 \\ d_2 & \text{if } u_1 = u_2. \end{cases}$$

$wt(x+y) \geq wt(x) + wt(y)$

$\Downarrow$

$= wt(u_1 - u_2) + wt(u_1 - u_2 + v_1 - v_2)$

$= wt(u_1 - u_2) + wt(v_1 - v_2)$

$= wt(v_1 - v_2) \geq d_2$.

- $C_1 (n, M_1, d_1)$, $C_2 (n, M_2, d_2)$

$$C_1 * C_2 = \{ u|u+v \mid u \in C_1, v \in C_2 \}.$$

$(2n,\ M_1 M_2,\ d = \min\{2d_1, d_2\})$ code.

$z_1 = u_1 | u_1 + v_1$ $\quad u_1, u_2 \in C_1$

$z_2 = u_2 | u_2 + v_2$ $\quad v_1, v_2 \in C_2$.

Case I: $v_1 = v_2$, $u_1 \neq u_2$

$\text{dist}(z_1, z_2) = 2\,\text{dist}(u_1, u_2) \geq 2d_1$

Case II: $v_1 \neq v_2$, $u_1 = u_2$

$\text{dist}(z_1, z_2) = \text{dist}(u_1, u_2) + \text{dist}(u_1 + v_1, u_2 + v_2)$

$= \text{dist}(v_1, v_2) \geq d_2$

- $\mathcal{C}_1, \mathcal{C}_2 \to$ linear with dimension k_1, k_2 resp^{ly}.

then $\mathcal{C}_1 \oplus \mathcal{C}_2$, $\mathcal{C}_1 * \mathcal{C}_2$ are also linear of dimension

$k_1 + k_2$ ↓ F_q^{2n} ↓ F_q^{2n}

$z_1, z_2 \in \mathcal{C}_1 \oplus \mathcal{C}_2$ over F_q or

$z_1 = u_1|v_1$, $z_2 = u_2|v_2$

$u_1, u_2 \in \mathcal{C}_1 \Rightarrow \alpha u_1 + \beta u_2 \in \mathcal{C}_1$

$v_1, v_2 \in \mathcal{C}_2 \Rightarrow \alpha v_1 + \beta v_2 \in \mathcal{C}_2$.

$\alpha z_1 + \beta z_2 = \alpha u_1 + \beta u_2 | \alpha v_1 + \beta v_2 \in \mathcal{C}_1 \oplus \mathcal{C}_2$.

$\alpha, \beta \in F_q$

⇓

$\mathcal{C}_1 \oplus \mathcal{C}_2$ is linear.

$M_1 = q^{k_1}$, $M_2 = q^{k_2}$

$\therefore M_1 M_2 = q^{k_1 + k_2}$

⇓

$\mathcal{C}_1 \oplus \mathcal{C}_2$ has dimension $k_1 + k_2$.

~~• $\mathcal{C}_1, \mathcal{C}_2 \to$ linear with dimension k_1, k_2 resp^{ly}.~~

~~then $\mathcal{C}_1 * \mathcal{C}_2$~~

$z_1, z_2 \in \mathcal{C}_1 * \mathcal{C}_2$

$z_1 = u_1 | u_1 + v_1$

$z_2 = u_2 | u_2 + v_2$

$u_1, u_2 \in \mathcal{C}_1$

$v_1, v_2 \in \mathcal{C}_2$

⇓

$\alpha u_1 + \beta u_2 \in \mathcal{C}_1$, $\alpha v_1 + \beta v_2 \in \mathcal{C}_2$

$\alpha, \beta \in F_q$

$\alpha z_1 + \beta z_2$

$= \alpha u_1 + \beta u_2 \mid \alpha(u_1 + v_1) + \beta(u_2 + v_2)$

$= \alpha u_1 + \beta u_2 \mid \alpha u_1 + \beta u_2 + (\alpha v_1 + \beta v_2)$

$\in \mathcal{C}_1 * \mathcal{C}_2$.

of codes

Prove that $n = n_1 + n_2$

$C_1 (n, M_1, d_1)$

$C_2 (n, M_2, d_2)$

u/v 1) $C_1 \oplus C_2$ is a $(2n, M_1 M_2, \min\{d_1, d_2\})$ code.

u/u+v 2) $C_1 * C_2$ is a $(2n, M_1 M_2, \min\{2d_1, d_2\})$ code. ($n_1 = n_2$)

3) If C_1, C_2 are linear of dimension k_1, k_2 respectively, then show that both $C_1 \oplus C_2$ & $C_1 * C_2$ are linear of dimension $k_1 + k_2$.

~~Reed-Muller~~

$C_1 = [4, 3, 2]$ even weight code $\rightarrow R(m-1, m)$ $\quad n = 2^m = 4 \neq m = 2$

$C_2 = [4, 1, 4]$ repetition code of length 4

$\rightarrow R(0, 2)$

then

$C_3 = C_1 * C_2 = [8, 4, 4]$ 1st order Reed-Muller code of length $8 = 2^3$.

$\rightarrow RM(1, 3)$ $\quad n = 8 = 2^3$.

$C_1 = [8, 4, 4] \rightarrow R(1, 3)$

$C_2 = [8, 1, 8]$ repetition code of length 8.

$\hookrightarrow R(0, 3)$

then

$C_3 = C_1 * C_2 = [16, 5, 8]$ 1st order Reed-Muller code of length $16 = 2^4$.

$C_1 = [16, 5, 8] \rightarrow R(1, 4)$ $\rightarrow RM(1, 4)$.

$C_2 = [16, 1, 16] \rightarrow R(0, 4)$ repetition code of length 16

$C_3 = C_1 * C_2 = [32, 6, 16] \rightarrow RM(1, 5)$. & so on.

Reed - Muller Codes

An r th order Reed-Muller code of length $n = 2^m$ is denoted by $RM(r, m)$ when $0 \le r \le m$, is defined inductively as follows:

1) $RM(0, m)$ is the binary repetition code of length $n = 2^m$.

2) $RM(m, m) = F_2^n$, $n = 2^m$

3) $RM(r, m) = RM(r, m-1) * RM(r-1, m-1)$ for any r, $0 < r < m$

Example. find $RM(1,2)$.

$RM(2,3) = RM(2,2) * RM(1,2)$

$RM(1,2) = RM(1,1) * RM(0,1)$.

Now, $RM(0,1)$ = binary repetition code of length $n = 2^1 = 2$

$= \{00, 11\}$.

$R(m,m) = F_2^m$

$RM(1,1) = F_2^n$, $n = 2^1$

$= F_2^2$

$= \{00, 01, 10, 11\}$

$R(0,m) = (\underbrace{00\cdots0}_{m}, \underbrace{11\cdots1}_{m})$

(Exercise) $R(m-1, m)$ → all even weight vectors.

$d = 2^{m-(m-1)} = 2$

As $C_1 * C_2 = \{x | x+y : x \in C_1, y \in C_2\}$.

Here $RM(1,2) = \{00, 01, 10, 11\} * \{00, 11\}$

$= 0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100\}$

$C_1 * C_2 = \{2, 6, 16\}$ → $RM(1,5)$. & so on.

ample

find RM(1,3)

We have

$$RM(1,3) = RM(1,2) * RM(0,2).$$

Now $RM(1,2) = \{0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100\}$.

and $RM(0,2)$ = binary repetition code of length $n = 2^2 = 4$

$= \{0000, 1111\}$.

Hence $RM(1,3) = \{00000000, 00001111, 00110011, 00111100, 01010101, 01011010, 01100110, 01101001, 10101010, 10100101, 10011001, 10010110, 11111111, 11110000, 11001100, 11000011\}$

Example

find RM(1,4)

$$RM(1,4) = RM(1,3) * RM(0,3). \qquad n = 2^3 = 8$$

$RM(0,3) = \{00000000, 11111111\}$.

$\therefore RM(1,4) = ?$

Example

$RM(3,3) = RM(2,2) * RM(1,2)$

F_2^n, $n = 2^2 = 4$

$= \{16$ elements (4 tuples)$\}$

$RM(2,4) = RM(2,3) * RM(1,3)$

$\rightarrow \ldots G_2 = [32, 6, 16] \rightarrow RM(1,5)$. & so on.

Show that $RM(r,m)$ is a binary linear code of dimension $k = \sum_{i=0}^{r} \binom{m}{i}$; min. dist. $d = 2^{m-r}$.

Length $n = 2^m$.

Proof by induction

$$RM(r,m) = RM(r,m-1) * RM(r-1,m-1)$$

dimension: k ↓ k_1 ↓ k_2

$$k = k_1 + k_2 .$$

$$k_1 = \sum_{i=0}^{r} \binom{m-1}{i} , \quad k_2 = \sum_{i=0}^{r-1} \binom{m-1}{i}$$

$$\therefore k = k_1 + k_2$$

$$= \sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i}$$

$$= \binom{m-1}{0} + \sum_{i=1}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} \qquad j = i+1$$

$$= 1 + \sum_{i=1}^{r} \binom{m-1}{i} + \sum_{j=1}^{r} \binom{m-1}{j-1}$$

$$= 1 + \sum_{i=1}^{r} \left[\binom{m-1}{i} + \binom{m-1}{i-1} \right]$$

$$= 1 + \sum_{i=1}^{r} \binom{m}{i} = \binom{m}{0} + \sum_{i=1}^{r} \binom{m}{i} = \sum_{i=0}^{r} \binom{m}{i}$$

min dist ↓ d ↓ d_1 ↓ d_2.

$$d = \min\{2d_1, d_2\}$$

$$d_1 = 2^{m-1-r}, \quad d_2 = 2^{m-r}.$$

$$\therefore d = \min\{2^{m-r}, 2^{m-r}\} = 2^{m-r}.$$

RM → one of the oldest & best understood families of codes.

→ relatively easy to decode (especially for 1st order RM code)
→ good practical codes & basis for constructing many other codes.

RM code of length 2^{m+1} may be obtained from RM codes of length 2^m using $|u|u+v|$ construction

Dual of
- $RM(r,m) \xrightarrow{\text{Dual}} RM(m-r-1, m)$, $0 \le r \le m-1$

proof.

- Decoding is especially easy for 1st-order RM codes.
- $R(r,m)$ can be easily encoded & decoded by majority logic.

- Defining RM codes using Boolean fn^n,

$RM(r,m)$, $n = 2^m$, $0 \le r \le m$; $v = (v_1, \ldots, v_m) \in V^m$

↖ Set of all vectors f, where $f(v_1, \ldots, v_m)$ is a B.F which is a poly. of deg. at most r.

$RM(1,3)$, $n = 2^3$ → codewords $a_0 1 + a_1 v_1 + a_2 v_2 + a_3 v_3$, $a_i = 0$ or 1

$R(1,3)$ codewords of length $n = 2^3 = 8$.

0	0	0	0	0	0	0	0
v_3	0	0	0	0	1	1	1	1
v_2	0	0	1	1	0	0	1	1
v_1	0	1	0	1	0	1	0	1
$f \rightarrow$	0	0	1	0	0	1	0	0
v_2+v_3								
v_1+v_3								
v_1+v_2								
$v_1+v_2+v_3$								
1								
$1+v_3$								
$1+v_2$								
$\vdots$								
$1+v_1+v_2+v_3$								

$f = \bar{v}_1 v_2 \bar{v}_3 + v_1 \bar{v}_2 v_3$ $\hookrightarrow$ deg 3.

# of codewords $= 2^{\binom{m}{r}} = 2^k = 2^4 = 16$

$k = \sum_{i=0}^{r} \binom{m}{i}$

$= 1 + \binom{3}{1}$

$= 1+3 = 4$.

$v = (v_1, \cdots, v_m) \in V^m$ (eg. $V = F$)

$f \rightarrow$ vector of length 2^m.
obtained from B.F. $f(v_1, \cdots, v_m)$

# of possible such $f \rightarrow 2^{2^m}$ $\Rightarrow$ all distinct.

deg 0: 1 — deg 1: $v_1, v_2, \cdots, v_m$ — deg 2: $v_1v_2, v_1v_3, \cdots, v_{m-1}v_m$, ... — deg m: $v_1 v_2 \cdots v_m$.

$\hookrightarrow$ linear combinations with coeff.'s 0 or 1.

$RM(r,m) \rightarrow 1, v_1, v_2, \cdots, v_m, \cdots$ upto degree r
$\rightarrow$ basis for the code

Th. $R^{\perp}(r,m) = R(m-r-1, m), \quad 0 \le r \le m$

Proof: $a \in R(m-r-1, m), \; b \in R(r,m)$

$\deg a(v_1, \cdots, v_m) \le m-r-1$

$\deg b(v_1, \cdots, v_m) \le r$

$\Rightarrow \deg ab \le m-1$

$\Rightarrow ab \in R(m-1, m)$, has even weight (Exercise)

$\therefore a \cdot b = 0 \pmod 2$

$\Rightarrow R(m-r-1, m) \subseteq R(r,m)^{\perp}$

Now $\dim R(m-r-1, m) + \dim R(r,m)$

$= \left\{1 + \binom{m}{1} + \cdots + \binom{m}{m-r-1}\right\} + \left\{1 + \binom{m}{1} + \cdots + \binom{m}{r}\right\}$

$= 2^m = $ length $R(r,m)$.

$\Rightarrow R(m-r-1, m) = R(r,m)^{\perp}$

$\mathcal{C} \to$ length n.

$\dim \mathcal{C} \to k$

$\dim \mathcal{C}^{\perp} \to n-k$.

$\dim \mathcal{C} + \dim \mathcal{C}^{\perp}$

$= n-k+k = n$

$=$ length $\mathcal{C}$