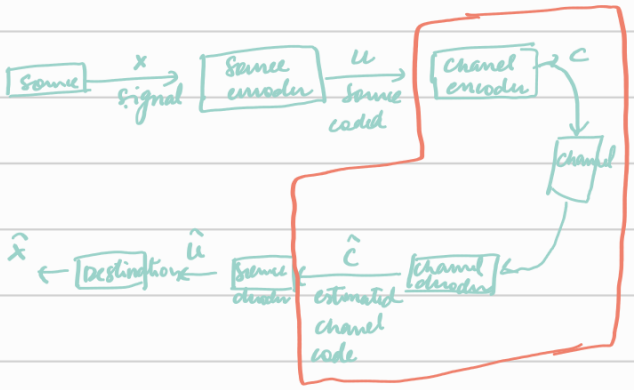
HW: 15%, Quizzes: 20%, M: 25%, E: 35%, Scribing: 5%



Channel model → Discrete

F → input alphabet

ϕ → output alphabet

$P_n(y_{recieved} \mid x_{transmitted})$

$(x, y) \in F^n \times \phi^n$

I/p to channel encoder (Encoder → Message, $m \in \{1, 2, \cdots, M\}$)

channel coder map m to codeword $c \in F^n$ (one-to-one map)

Recieved o/p → $y \in \phi^n$. Decoder generates $\hat{c}$ → decoded codeword

(n, M) code

Rate: $R \triangleq \frac{\log_{|F|} M}{n} = \frac{\log_2 M}{n \log_2 |F|}$ ← amount of information in bits; ← amount of bit communicating

Example: $M = 4$ $\{1,2,3,4\}$, $F = \phi\{0,1\}$

$n = 5$ ↑ binary string of length 5

m
(00) 1 → 10101
(01) 2 → 10010
(10) 3 → 01110
(11) 4 → 11111
k=2, n=5

$\text{Rate} = \frac{\log 4}{5 \times \log 2} = 0.4$

(k, n) code rate = $\frac{k}{n}$

Uncoded transmission → $F = \{0,1\}$, $n = 1$

$M = \{0,1\}$ (↓ 0, ↓ 1), $R = \frac{1}{1} = 1$ → No error correcting capability

Repetition code → $M = \{0,1\}$ $0 \to \underbrace{0000}_{n}$ $R = 1/n$

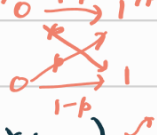
$1 \to 1111$

Majority decoder. Error correcting capability ~ $\frac{n}{2}$ errors

Channels:

Eg → Memoryless Binary Symmetric channel (BSC)

← flips the bit with probability p.



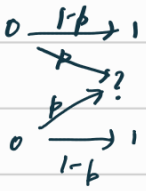
$P(y \text{ recieved} \mid x \text{ tr}) = \prod_{i=1}^{n} P(y_i \text{ recieved} \mid x_{trans})$ ↗ $\begin{cases} P, \text{ incor} \\ 1-p, \text{ corr} \end{cases}$

memoryless 2 sym. channel

x_i tx	y_j	
	$y_j = x_i$	$1-p$
	$y_j \neq$	$\frac{p}{q-1}$

Memoryless Binary Erasure channel (BEC)

$F = \{0,1\}$, $\emptyset = \{0,1,?\}$



Decoding

A decoder is a func. $D: \emptyset^n \to C$

Error probability $P_e(c) = P(\hat{c} \neq c)$

$= \sum_{y_i \; D(y) \neq c} P(y \neq x \mid c_{tx})$

$P_e \triangleq \max P_e(c)$

BSC (p)

→ uncoded $k=1$, $n=1$, $P_e = p$

→ Repetion code $k=1$, n

Majority decoder

{000, 100, 001, 010} → 1

{111, 011, 101, 110} → 2

P_e = P(≥2 errors were introduced by channel)

$= {}^3C_2 (p-1) p^2 + p^3$

Coding for storage

→ Simple parity check code

$k=2$, $n=3$

cannot correct errors, (not enough redundancy is introduced)

00 → 000

01 → 011

10 → 101

11 → 110

redundancy

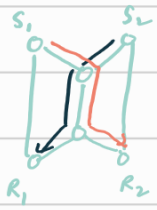
$R = 2/3$

0 error correction

1 error detection

Network coding

→ $R = 1$

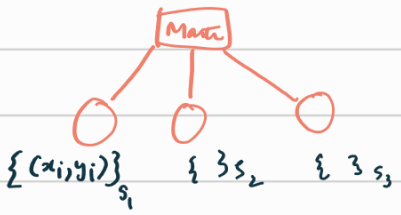


$R = 1/2$

$\{ S_1 \to R_2 \;\; S_2 \to R_1 \}$ (via x)

Coded Computing

$$\beta^* = \arg\min_{\beta} \sum_{i=1}^{n} L(x_i, y_i, \beta)$$



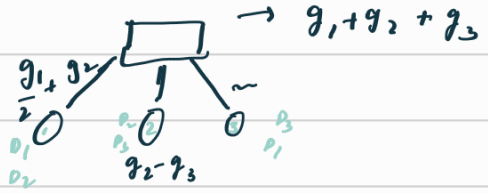
$$\sum_{i=1}^{n} \nabla L(x_i, y_i, \beta^{t-1})$$

(Gradient Coding)

if redundancy is not there, directly partioning the whole set.

↳ Then will wait for each to compute

$D = D_1 \cup D_2 \cup D_3$



Even if one of servers fail, we still can do.

Block Code

Finite Alphabet F ; (n, M) block code is a subset $C \subseteq F^n$, $|C| = M$

$n \rightarrow$ code length, $C \rightarrow$ code, Elements of C are called codewords

$K \rightarrow \log_{|F|} M$, Rate $R = \frac{K}{n}$

Hamming distance : $x, y \in F^n$ $d_H(x, y) \rightarrow$ # positions where x, y differ

(Valid metric): ① $d(x,y) \geq 0$ ② $d(x,y) = d(y,x)$ ③ Δ ineq: $d(x,y) \leq d(x,z) + d(z,y)$

Minimum distance of code C $= \min_{x,y \in C} d(x,y) \triangleq d(C)$

n, M, d

Repetion code : $(3, 2, 3)$ code

111
000

Simple parity check : $(3, 4, 2)$ code

Error Correction

Claim : An (n, M, d) code can correct all error pattern which have atmost $\lfloor \frac{d-1}{2} \rfloor$ errors.

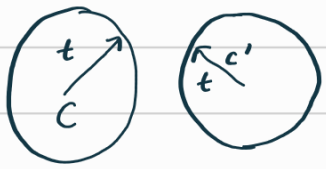
Pf : Minimum distance decoder $D(y) = \arg\min_{c \in C} d(c, y)$

(contray) Assume C was transmitted and y recieved s.t. $d(c, y) \leq \lfloor \frac{d-1}{2} \rfloor$

and yet $\exists\ c' \neq c$, $d(y,c') \leq d(y,c)$

$d(c,c') \leq d(c,y) + d(y,c') \leq \lfloor \frac{d-1}{2} \rfloor \times 2 \leq d-1$

$\Rightarrow$ Contradiction



(How can one prove the converse ?)

for any codebook, any decoder, with some error pattern $> \lfloor \frac{d-1}{2} \rfloor$

Error detection

Claim → An (n, M, d) code can detect any error pattern upto $d-1$ errors. $D(y) = \begin{cases} c & \text{if } y = c \\ \text{error} & \text{o.w.} \end{cases}$

Error correction + detection

Claim → $\exists\ t, \ell$ s.t. $\boxed{2t + \ell \leq d-1}$, upon (n, M, d) code

→ if # of errors $w \leq t$, error will be corrected

→ if # errors $\leq t+\ell$, error pattern will be detected

Pf: $D(y) = \begin{cases} c & \text{if } c \in C,\ d(y,c) \leq t \\ \text{err} & \text{o.w.} \end{cases}$

$t \leq \lfloor \frac{d-1}{2} \rfloor$ so all error patterns upto t errors will be corrected.

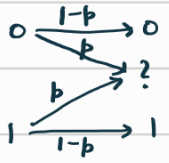
$\exists\ c_x, y_x$ s.t. $d(y,C) \leq t+\ell$

Error will not be detected if y lies within distance t of $c' \neq c$

$d(y, c') \leq t$

$d(c, c') \leq 2t+\ell \leq d-1$ ← contradiction

Erasure Correction



Claim: An (n, M, d) code can correct upto $d-1$ erasures.

Pf: Decoding rule: $D(y) = \begin{cases} c & \text{if } c \text{ is the unique codeword that agrees with } y \\ \text{error} & \text{o.w.} \end{cases}$

Assume the contary $\exists\ c, c'$ $c \neq c'$ both agreing with y.

$\Rightarrow d(c, c') \leq d-1 \Rightarrow$ contradiction.

(n, M, d) code over a channel which introduces errors & erasures

$2t + l + s \leq d-1$, then for s erasures where $0 \leq s \leq d-1$

① If # errors $\leq t$, then recovery feasible

② O/w, if # errors $\leq t+l$, then errors will be detected.

Linear Codes

(Order of Group = No. of elements)

Group: set with (binary) operation $(*)$ {Closure, Associativity, Identity (e), Inverse}

Abelian group: commutative Group

Subgroup: If a subset is a group.

Subgroup Construction: $h \in G$, G is finite

$\{h, h*h, h*h*h, \cdots\}$

↖ 1st element to be repeated will be h, as G is finite

Assuming contrary: $h^i = h^j \quad 1 \leq i < j$

$\Rightarrow h^{i-1} = h^{j-1} \Rightarrow$ contradiction

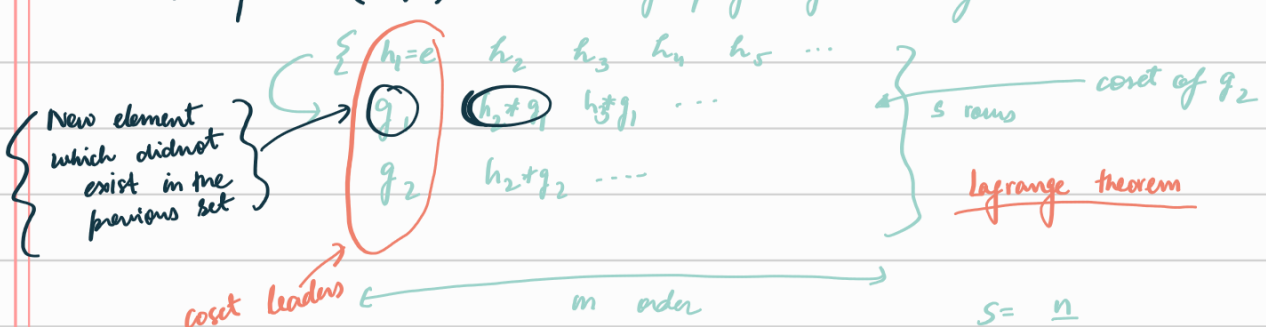
$H = (h, h^2, h^3, \cdots, h^{j-1} = e)$ ← cyclic subgroup

↑ subgroup spanned by h.

$G = \{0, 1, 2, \cdots, 8\}$ $\quad * =$ mod-9 addition

$h = 3 \quad H = \{3, 6, 0\}$ ← order = 3

Coset decomposition (G/H): H is subgroup of G generated by h. → $\{e, h_1, \cdots, h_{m-1}\}$



Claim: Each element occurs exactly once in the coset decomposition.

Pf: Two elements in the same row are repeated

$g_i * h_j = g_i * h_k \Rightarrow h_j = h_k \Rightarrow$ Not true

{multiplication with inverse}

Rows $a, b \quad a > b$ Repetition of elements

$g_a * h_i = g_b * h_j$

$$g_a * h_i * h_i' = g_b * \underbrace{h_b * h_i'}_{\in H}$$

$$\Rightarrow \quad g_a = g_b * h \quad \Rightarrow \text{ contradiction}$$

Lagrange Thm Corrolary: m divides n.

Field: A field F is a set of elements with two binary operation $(+)$ & $(\cdot)$

① F is abelian group wrt $\oplus$ ← 0 additive identity

② F is closed under $\odot$

& non-zero elements form an abelian group under $(\cdot)$ (mult. identity 1)

③ Distributive law holds

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

GF(2): $\{0,1\}$ with mod-2 addition & multiplication

GF(N): with mod-N addition & multiplication. It is a field when $N = p$ is prime.

↑ Galois field → $N = p^m$ GF(4) or of form $N = p^m$

Galois Field (4)

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Vector field: V: On a field F, ∃ vector addition & scalar multi

① V is abelian group under $\oplus$

② $\forall a \in F, v \in F \Rightarrow a \cdot v \in V$

③ $a(v_1 + v_2) = av_1 + av_2$

④ $(a_1 + a_2)v = a_1 v + a_2 v$

⑤ $(a_1 a_2) \cdot v = a_1 \cdot (a_2 v)$

⑥ $1 \in F$, be multi identity, $1 \cdot v = v$

↝ To show: $\vec{0}$ is additive identity for vectors

(a) $0 \cdot v = \vec{0}$ (b) $c \cdot \vec{0} = \vec{0}$ (c) $(-c) \cdot v = c \cdot (-v) = -(c \cdot v)$

Proof: (a) $0 \cdot v = (0+0) \cdot v = 0 \cdot v + 0 \cdot v$

$\Rightarrow$ $0 \cdot v$ is additive identity $= \vec{0}$

(b) $c \cdot \vec{0} = c \cdot (0 \cdot v) = (c \cdot 0) \cdot v = 0 \cdot v = \vec{0}$

(c) $(c + (-c))v = \vec{0}$

$\Rightarrow$ $cv + c(-v) = 0 \quad \Rightarrow \quad -v = c(-v)$

$(-c) \cdot v + c \cdot v = 0 \cdot v = \vec{0} \Rightarrow (-c)(v) = -(c \cdot v)$

Subspace: V is V.S., $U \subseteq V$ s.t.

- $u \in U, v \in U \Rightarrow u + v \in U$
- $a \in F, v \in U \Rightarrow a \cdot v \in U$

Eg : { (00000), (00111), (11010), (11101) is a subspace of $[GF(2)]^5$ }

Linear Independence : $v_1 \dots v_k \in V$ & $\sum a_i v_i = 0 \Rightarrow a_i = 0 \ \forall i$, then lin indep

Basis — Spanning & Lin Indep

Inner product : $\langle \cdot, \cdot \rangle : V \times V \to F$ is an inner product if

(a) $\langle v, v \rangle \geq 0$ & $\langle v, v \rangle = 0 \iff v = \vec{0}$

(b) $\langle v, u \rangle = \langle u, v \rangle$

(c) $\langle av, u \rangle = a \langle v, u \rangle$

Orthogonal : $\langle v_1, v_2 \rangle = 0$

$W^\perp$: Set of vectors orthogonal to all vectors w_j

Eg. (1,1) is orthogonal to itself $\langle (1,1), (1,1) \rangle = (1 \cdot 1) \oplus (1 \cdot 1)$
$= 0$

Bitwise "and", followed by XOR

$W = \{ (0,0), (1,1) \}$

$W^\perp = \{ (0,0), (1,1) \}$

$\dim W + \dim W^\perp = 2$

$W = \{ (000), (101), (001), (100) \}$, $W^\perp = \{ 000, 010 \}$

$\dim (W) = 2$, $\dim W^\perp = 1$

Matrices : kxn matrix over a field F.

$M = \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & \dots \end{bmatrix}$ ($f_{ij} \in F$), k rows, n columns, $k \times n$

{ #rows x #columns }

GENERATOR MATRIX of a code : Matrix whose row space spans the code ($\subseteq$ subspace)

$G \in F^{k \times n}$, rowspace $(G) = W$

If $\dim (W) = k$ then $\dim (W^\perp) = n - k$

define $H \in F^{n-k \times n}$, such that rowspan $(H) = W^\perp$

$\therefore$ By orthogonality we have :

$GH^T = 0$

We will only deal with linear codes that are subspaces. Code has

a generator matrix G & parity check matrix H. we have $GH^T = 0$.

BLOCK LINEAR CODES

(n, m, d) code over F is called linear if C is a subspace of F^n.

If $\dim(C) = k$, then $|M| = |F|^k$ $\therefore R = \frac{k}{n}$

Eg. Parity check code : $(3,4,2)$

$\{000, 011, 110, 101\}$

$\dim = 2$, Rate $= \frac{2}{3}$, $G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$, $H = [1\ 1\ 1]$

Eg. Repetition code : $(3,2,3)$ $\{000, 111\}$

$\dim = 1$, Rate $= 1/3$, $G = [1\ 1\ 1]$, $H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

Minimum distance

$$d = \min_{\substack{c \in C \\ c \neq \vec{0}}} w(c)$$ ← Hamming weight of C = # of non zero entries

Proof : If $a, b \in C$, $a \neq b$

$d(a,b) = w(a \oplus b)$, Now $a \oplus b \in C$

$$\therefore \min_{\substack{a \neq b \\ a,b \in C}} d(a,b) = \min_{\substack{c \in C \\ c \neq \vec{0}}} w(c)$$

Generator matrix can be used as encoder

Message size: q^k over $GF(q)$ $\quad \mu_i \in GF(q)$

$\mu = [\mu_1 \cdots \mu_k]$

Message $= \mu G$ (G ↑ generator matrix)

(n, k) → n : length of code; k : dimension of the block code

Eg $(7,4)$ – Hamming code $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [I_{k \times k}\ A_{k \times (n-k)}]$ $k \times n$ (I: $k \times k$)

Such are called $k \times k$ systematic codes.

First k bits are message bits

$[\mu_0\ \mu_1\ \mu_2\ \mu_3]\ G \Rightarrow 5^{th}$ column is $\mu_0 + \mu_2 + \mu_3$

The parity check matrix is $[-A^T \mid I]$ $(n-k) \times n$ (I: $(n-k) \times (n-k)$)

$k \times (n-k)$ $\begin{bmatrix} -A \\ I \end{bmatrix}$ $[I_{k \times k}\ A]$

→ For a (n, k, d) block code with parity check matrix H, we have (the minimum distance d is the largest integer s.t. any $(d-1)$ columns of H are lin. ind.)

Proof: If min distance $= d \Rightarrow \exists\ c \in C$ s.t. $w(c) = d$

Then $Hc^T = 0$ ∴ those 'd' columns of H add to 0.

Also if $\exists\ c$ s.t. $0 < w(c) \leq d-1$ & $Hc^T = 0 \rightarrow c \in C$, but C is $(n, k, d) \Rightarrow$ contradiction.

Decoding of linear codes:

Given an (n, k, d) linear code $t_x : C$, $r_x : r = c + e$ ← error

decoded into $\hat{c}$

To decode, we use the coset decomposition of F^n over the subgroup – codewords

c_0	c_1	c_2	...	c_{q^k-1}
$e_1 + c_0$	$e_1 + c_1$			
$e_2 + c_0$	⋮			
⋮				
$e_{q^{n-k}-1}$				

q^k, total $= q^n$, leaders $= q^{n-k}$

Strategy is to map each $r = c + e$ to the codeword in the corresponding to its column in the coset decomposition

Appropriate coset leaders need to be chosen.

We can correct e iff it is a coset leader.

Proof: If e is a coset leader then $c_j + e$ lies in the same column as c_j ∴ correct decoding

If e is not a coset leader, then let the coset leader for e, $c_j + e$ be e_ℓ, then $c_j + e$ gets mapped to $c_j + e - e_\ell$ → incorrect

∴ we can correct q^{n-k} out of q^{nk} possible error patterns

So, if we have knowledge of the error patterns that we expect to see, we take them as coset leaders.

For nearest neighbour decoding, we use patterns like:

$(00\ldots01, 00\cdots010, \ldots$

$00\cdots011, 00\cdots0101, \ldots)$

Standard array decoding:

At each row i, choose the lowest available hamming weight vector as coset leaders. This corresponds to nearest neighbour decoding

Proof: Let $e_1, \dots$ be the coset leaders. Let $r = e_\ell + c_j$

Then $d(r, c_j) = w(e_\ell)$

Also $\forall\ c_i \neq c_j$

$$d(r, c_i) = w(e_\ell + c_i - c_j)$$

$\in$ coset (c_ℓ)

$$\geq w(e_\ell) \text{ by construction}$$

$$\geq d(r, c_j)$$

For a (n,k,d) linear code, and $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, all n-tuples of hamming weight $\leq t$ are coset leaders in standard array.

Pf: x, y $\quad w(x), w(y) \leq t \Rightarrow$ x & y cannot be in the same coset.

Contrary: they belong in the same

$\Rightarrow x - y \in C \quad wt(x-y) = d$

But $wt(x-y) \leq wt(x) + wt(y) = 2t \leq 2\left\lfloor \frac{d-1}{2} \right\rfloor < d$

q^{n-k} errors can be corrected

Error detection

- Errors which can't be found will be $\underset{\in C}{c_1} - \underset{\in C}{c_2} \in C$

Error pattern detected: $q^n - q^k$

(n,k,d) linear code

$$P(\text{Error detection}) = 1 - P(\text{error} \in \mathbb{C})$$

$$= 1 - \sum A_i p^i (1-p)^{n-i}$$

A_i = # of codewords in C with weight i

P(error correction using coset decoder) $\leftarrow$ when error is from the coset leader

$$= \sum \alpha_i p^i (1-p)^i$$

α_i = # coset leaders with weight i

Coset decomposition of (n,k,d)

$\nwarrow q^{n-k} \times q^k \leftarrow$ matrix size

Syndrome decoding

Received x, Syndrome $\underset{(1\times n-k)}{S} = \underset{(1\times n)}{x}\ \underset{(n\times n-k)}{H^T}$

① Syndrome of $c \in \mathcal{C}$ $= 0$

② All the vectors in any coset will have the same syndrome

ℓ^{th} coset $\rightarrow (e_\ell + C)$ $\quad s = (e_i + c) H^T = e_i H^T$

③ Diff cosets will have diff syndromes

$(e_1 - e_2) H^T = 0 \Rightarrow (e_1 - e_2)$ is a Codeword

Coset leaders	Syndromes
e_0	S_0
e_1	S_1
⋮	⋮
$e_{q^{n-k}}$	$S_{q^{n-k}}$

(now is it stored)

① Calculate $S = xH^T$

② Use table to find corresponding coset leader

③ $\hat{c} = x - e_\ell$

Eg. $(5, 2, 3)$ code

Imp. Lin. codes

① Parity check codes $(k, k+1, 2)$

$G = \underset{k}{[}\ I_k \ \big|\ \vdots \ ]$ $\quad H = [1\ 1\ 1\ \cdots\ 1]$

Repetion code — dual of parity check

② Hamming code on GF(2) $\quad (7, 4, 3)$ - code

$m \geq 1$

$(2^m - 1,\ 2^m - m - 1,\ 3)$

$H = \underset{m}{[}\ \underbrace{\begin{matrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{matrix}}_{2^m - 1} \ \big|\ \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \ ]$

$-A^T \mid I$

some d lin-dep, all $d-1$ lin-indep

Choose 2 1^{st}, add obtain 3^{rd}

$\Rightarrow$ These three will be lin dep. $\Rightarrow d = 3$

Decoding : Syndrome :

$q^{n-k} = 2^m$

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

# of vectors with weight $\leq t = 2^m$

Perfect code $\rightarrow$ satisfy hamming equality

↳ $|C| \leq \dfrac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$ holds for any code

They are very rare : $(2^m-1,\ 2^m-m-1,\ 3)$

q-ary Hamming code – GF(q)

Parity check matrix — $n \to$ every pair of columns is lin. ind.

$$\left[\underbrace{\frac{q^m-1}{q-1}}_{n},\ \underbrace{\frac{q^m-1}{q-1}-m}_{k},\ \underbrace{3}_{d}\right]$$

Choose all non zero m-tuple vectors which have 1 as the first non zero component

$q=3,\ m=3 \Rightarrow n=13,\ k=10,\ d=3$

Parity Matrix :

$$3\begin{bmatrix} 0&0&1&0&0&1&1&1&1&1&1&1&1 \\ 0&1&0&1&1&0&0&1&1&1&2&2&2 \\ 1&0&0&1&2&1&2&0&1&2&0&1&2 \end{bmatrix}$$

↑ every pair is lin indp.

& there are a total of $\left\{\frac{q^m-1}{q-1}-m\right\}$

Decoding by syndrome decoding

$$S = Hx^T$$

$C = (7,4,3)$ – HC

$$H = \underbrace{\left[\begin{array}{c|c|c} 1&0&1 & 1&1&0&0 \\ 1&1&0 & 1&0&1&0 \\ 0&1&1 & 1&0&0&1 \end{array}\right]}_{3\times 7} \qquad \underbrace{-A^T_{3\times 4}}\quad \underbrace{I_{3\times 3}}$$

$$G = \underbrace{\left[\begin{array}{c|c} I_{4\times 4} & A_{4\times 3} \end{array}\right]}_{4\times 7}$$

$$C = [u_0\ u_1\ u_2\ u_3\ P_0\ P_1\ P_2]$$

$$P_0 = u_0 + u_2 + u_3$$

$$P_1 = u_0 + u_1 + u_2$$

$$P_2 = u_1 + u_2 + u_3$$

Hamming syndrome table of the form

$$\begin{matrix} \text{LSB} \\ \\ \text{MSB} \end{matrix}\begin{bmatrix} 1 & 0 & \cdots \\ 0 & 1 & \cdots \\ 0 & 0 & \cdots \end{bmatrix}$$

↓

Gives the corresponding integer position of the flipped bit.

$C = 1\,0\,1\,0\,1\,0\,1$

$r = 1\,0\,0\,0\,1\,0\,1 \Rightarrow \text{syn} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$ → flipped bit

HC cannot detect K correct. $(2^m-1,\ 2^m-m-1,\ 3)$

Extended HC: $(2^m,\ 2^m-m-1,\ 4)$ $\longrightarrow$ $H_{old} = m\,[\ \ ]$ (with 2^m-1 columns)

Correct single error

Apply same (n, k, d^*)
$\downarrow$
$(n+1, k, d^*+1)$

$$H_{new} = (m+1)\begin{bmatrix} 1 & 1 \cdots 1 \\ 0 & \\ 0 & H_{old} \\ 0 & \end{bmatrix} \quad (2^m \text{ columns})$$

Introduce one overall parity bit on the msb

$(7,4,3) \rightarrow (8,4,4)$
$\uparrow$ self dual code

Modifications

1. Expanding / Extending → Increasing n by adding parity check symbols
   $n{+}{+},\ k$

2. Puncturing → Reduce n by doing some parity checks
   $n{-}{-},\ k$

3. Lengthening → Increase n, k, $n-k$ = same by adding info symbols
   $n{+}{+},\ k{+}{+}$

4. Shortening → Drop info symbols
   $n{-}{-},\ k{-}{-}$

Eg: $(7,4,3)$ HC

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

Remove column (4th column circled)

$n=6$
$$H \rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \Big\} k$$

$(6, 3, 3)$ ← least number of lin. dep. columns

Delete all even weight columns:
$$H \rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$
$(4,1,4)$ repetition code

Shortening Hamming Code

↳ $(2^m-1,\ 2^m-m-1,\ 3)$ $\{n-k = \text{same}\}$

$\downarrow$ we drop even weight columns (dropped 2^{m-1}).

New $H \rightarrow$ all odd weighted m length vectors in the columns

$m\,[\ \ ]$ (2^m-1 columns) $\rightarrow$ $m\,[\ \ ]$ ($2^{m-1}-1$ columns)

distance ≥ 3 (because all are odd) sum can't be even

New code : $(2^{m-1}-1,\ 2^{m-1}-m-1,\ 4)$ distance ≥ 4 (because take 1st three and find the sum)

$\Rightarrow$ distance $= 4$

⑤ Augmenting — Increase k, n unchanged — $n, k{+}{+}$

⑥ Expurgating — Decrease k, n unchanged — $n, k{-}{-}$

Expurgating HC → adding all 1 to H

$H' \rightarrow$ [1 1 1 1 1] $n-k+1$ $n-(k-1)$

$2^m-1,\ 2^m-m-2,$

All odd weight codewords are removed

$(2^m-1, 2^m-m-2, 4)$

Reed Muller Code (m, r) $0 \leq r \leq m$

(Lin Costello)

r^{th} order $RM(r,m)$

$n = 2^m,\ k = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r} = \sum_{i=0}^{r}\binom{m}{i},\ d = 2^{m-r}$

Example: $m=5, r=2 \Rightarrow n=32,\ k = 1+5+10 = 16,\ d=8$

$(32, 16, 8)$ - code

$m=5, r=3 \Rightarrow n=32,\ k=26,\ d=4$ $(32,26,4)$

Generator matrix of $RM(r,m)$

$G = \begin{bmatrix} G_0 \\ G_1 \\ \vdots \\ G_r \end{bmatrix}$

$G_0 \rightarrow$ All 1s vector of length 2^m 1×2^m

$G_1 \rightarrow \binom{m}{1} \times 2^m$ All binary tuples of length m as columns in columns in G

G_1: [ ] $\}m$ under 2^m

$G_2 \rightarrow \binom{m}{2} \times 2^m$ Take all pairs of rows from G_1 and include their product in G_2

$G_l \rightarrow \{\binom{m}{l} \times 2^m\}$ Take all possible l rows from G_1 & include their product

$(m=4, r=2)$

$n=16$ $(16, 11, 4)$

All codewords of RM have even weight

$RM(0,m) \subset RM(1,m) \subset \cdots$

Recursive Construction of G of RM (r, m)

↳ const. codeword of length 2^m for RM(r, m) from codewords of length 2^{m-1} → G (RM (r, m−1)), G (RM (r−1, m−1))

$1 \le r \le m$

$$RM(r,m) = \{ (u,\ u+v) \mid u \in RM(r,m-1),\ v \in RM(r-1,m-1) \}$$

$$G(r,m) = \begin{matrix} \Sigma_r^{m-1} \\ \Sigma_{r-1}^{m-1} \\ \Sigma_r^m \end{matrix} \begin{bmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \\ \underbrace{\qquad}_{2^{m-1}} & \underbrace{\qquad}_{2^{m-1}} \end{bmatrix}$$

Dimension of code: $(u, u+v)$ is a one to one map

Induction : Assume $\dim = 1 + \binom{i}{1} + \binom{i}{2} + \cdots + \binom{i}{r}$ for all $i \le m-1, r$

$|RM(r,m)| = |RM(r,m-1)| + |RM(r-1,m-1)|$ as it is a one to one map.

$= 1 + \binom{m-1}{1} + \binom{m-1}{2} + \cdots + \binom{m-1}{r}$

$1 + \binom{m-1}{1} + \cdots + \binom{m-1}{r-1}$

$= 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$

[use $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$]

Min. Dist : of $RM(r,m) = 2^{m-r}$

$m=1 \xrightarrow{r=0} (00, 11) \rightarrow d = 2 = 2^{m-r}$

$\xrightarrow{r=1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$ $d^{\perp} = 1 = 2^{m-r}$

Assume $d = 2^{i-r}$ for all $i \le m, r$ show that holds true for $m+1$

$f, f' \in RM(r,m)$; $g, g' \in RM(r-1, m)$

RM $(r, m+1)$: $c_1 = (f,\ f+g)$ $c_2 = (f',\ f'+g')$

$g = g'$, $d(c_1, c_2) = 2\,d(f, f') \ge 2^{m+1-r}$

$w(x+y) \ge w(x) - w(y)$

otherwise : $d(c_1, c_2) = w(f-f') + w(f-f'+g-g')$

$\ge w(f-f') + w(g-g') - w(f-f') \ge 2^{m+1-r}$

Dual code of RM(r,m) is RM(m-r-1, m)

RM(0, m) – Repetition code

dual → RM(m-1, m) – Simple parity check code

$n = 2^m$

$k = 1 + \binom{m}{1} + \binom{m}{2} \cdots \binom{m}{m-1} = 2^m - 1$ {length + distance}

$m=2$ RM(0,2) ; RM(1,2)

Code word $\{0000, 1111\}$

$G = [1111]$ 1×4

$\hat{G} = \begin{bmatrix} 1&1&1&1 \\ 0&0&1&1 \\ 0&1&0&1 \end{bmatrix}$ 3×4

$G\hat{G}^T = 0$ & dim G + dim $\hat{G}$ = n = 4

Assume true for m-1, for all r

$$G_{r,m} = \left[\begin{array}{c|c} G_{r,m-1} & G_{r,m-1} \\ \hline 0 & G_{r-1,m-1} \end{array}\right] \qquad \begin{matrix} a & a \\ & \\ o & c \end{matrix}$$

$$G_{m-r-1,m} = \left[\begin{array}{c|c} G_{m-r-1,m-1} & G_{m-r-1,m-1} \\ \hline 0 & G_{m-r-2,m-1} \end{array}\right] \qquad \begin{matrix} b & b \\ & \\ o & d \end{matrix}$$

① (a|a) ⊥ (b|b) ② (a|a) ⊥ (0|d) ✓

③ (0|c) ⊥ (b|b) ← From induction ④ (0|c) ⊥ (0|d) ✓

From induction, we know: $G_{r,m-1} \perp G_{m-r-2,m-1}$; $G_{r-1,m-1} \perp G_{m-r-1,m-1}$

① → Holds : $(a \cdot b) \oplus (a \cdot b) = 0$

We need: ② $(r,m-1) \perp (m-r-2, m-1)$ ✓ & ③ $(r-1, m-1) \perp (m-r-1, m-1)$ ✓ & ④ $(r-1, m-1) \perp (m-r-2, m-1)$ ✓

$G_{r-1,m-1}$ is a subspace of $G_{r,m-1}$

$G_{m-r-2,m-1}$ is a subspace of $G_{m-r,m-1}$

$$G^* = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$G^* \circledast G^* = \begin{bmatrix} 1&1&1&1 \\ 0&1&0&1 \\ 0&0&1&1 \\ 0&0&0&1 \end{bmatrix}$$

$(G^*)^m \rightarrow \binom{m}{l}$ rows of weight 2^{m-l}

RM(r,m) → Take rows of $(G^*)^m$ with wt $\geq 2^{m-r}$

Decoding $\left(\frac{2^{m-r}}{2} - 1\right)$ errors based on majority decoding

Assume existence for RM(r-1, m) which can correct upto $\left(\frac{2^{m-(r-1)}}{2} - 1\right)$ errors

Base case : RM(0,m) → $2^{m-1} - 1$ error repetition code

$[\bar{u}_0 \quad \bar{u}_1 \quad \bar{u}_2 \quad \cdots \quad \bar{u}_{r}]$ — collecting the message bits together

$u_0 \; u_1 \; u_2 \; \cdots \; u_{K-1}$

$$\begin{bmatrix} G_0 \\ G_1 \\ \vdots \\ G_{r-1} \\ G_r \end{bmatrix}$$

Focus on decoding $\bar{u}_r$

$v = c + e$

$v' = c + e - \bar{u}_r \cdot G_r$ → can be decoded using RM $(r-1, m)$ decoder

How to get $\{u_{K-1}\}$

Create: 2^{m-r} parity check each of which will consist of 2^r received symbols with no overlap

In each parity

→ u_{K-1} contribute once to symbols in parity

→ All other message bits contribute an even # times

Use a majority decoder on this parity checks.

No overlap ⇒ a maximum of $\frac{2^{m-r}}{2}$ will have error, these still can decode

(2,4) RM code

↳ (16,11) code

$[\bar{u}_0 \; \bar{u}_1 \; \bar{u}_2]$

$[u_0 \; u_1 \; \cdots \; u_{10}]$

$$\begin{bmatrix} G_0 \\ G_1 \\ G_2 \end{bmatrix}$$

$1 \; [u_0 \; u_1 \; \cdots \; u_{K}]$

$u \; G$

$1 \times 11 \quad 11 \times 16$

16

$$\begin{bmatrix} 1\,1\,1\,1 & & & \\ 0\,0\,0\,0 & & & \\ 0\,0\,0\,0 & & & \\ 0\,0\,1\,1 & & & \\ 0\,1\,0\,1 & & & \\ 0\,0\,0\,0 & & & \\ 0\,0\,0\,0 & & & \\ 0\,0\,0\,0 & & & \\ 0\,0\,0\,0 & & & \\ 0\,0\,0\,1 & & & \end{bmatrix} \begin{matrix} G_0 \\ \\ \\ \\ G_1 \\ \\ \\ \\ G_2 \\ \\ \end{matrix}$$

adding these 4 columns we get $\begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$

$$4 \begin{bmatrix} 1\,1\,1\,1 & 0\,0\,0\,0 & & \\ 0\,0\,0\,0 & 1\,1\,1\,1 & 0 & \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 1\,1\,1\,1 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 1\,1\,1\,1 \end{bmatrix} \begin{bmatrix} \\ \\ \\ \\ \end{bmatrix} 1$$

16 16

$p_1 = v_0 + v_1 + v_2 + v_3$

$p_2 = v_4 + v_5 + v_6 + v_7$

$p_3 = v_8 + v_9 + v_{10} + v_{11}$

$p_4 = v_{12} + v_{13} + v_{14} + v_{15}$

Rep code — $(n, 1, n)$ code

Simple parity $(n, n-1, 2)$ code

Hamming $(2^m - 1, 2^m - m - 1, 3)$: $m \geq 2$

RM code $\left(2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}\right)$: $m \geq 1$, $0 \leq r \leq m$

(n, k, d)

Sphere packing / Hamming bound

For any (n, M, d) code over an alphabet of size q

$$M \leq \frac{q^n}{Vol_q\left(n, \left\lfloor \frac{d-1}{2} \right\rfloor\right)}$$

$$Vol_q(n,t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

If linear, $M = q^k$

$A_q(n, d) \rightarrow$ maximum size of code over $GF(q)$ with length n & min dist. d

Singleton Bound

For any (n, M, d) code over an alphabet of size q

$$d \leq n - \lceil \log_q M \rceil + 1 \quad \text{or} \quad M \leq q^{n-d+1}$$

lin code $\Rightarrow$ $d \leq n - k + 1$

Pf: $\ell = \lceil \log_q M \rceil - 1 \Rightarrow q^\ell < M$ {largest ℓ st $q^\ell < M$}

For the first ℓ positions we have q^ℓ holes & M pigeons $\Rightarrow \exists$ atleast 2 codewords which agree on the first ℓ symbols. {From Pigeon-hole Principle}

$$\Rightarrow d \leq n - \ell = n - \lceil \log_2 M \rceil + 1$$

For lin code:

For H, any $d-1$ columns are lin. indep.

$$d - 1 \leq n - k$$

$d = \text{rank} + 1$

$$\text{rank} \leq n - k$$

$$d \leq n - k + 1$$

Generator matrix: in systematic form, always has: $G = k \left[I_k \;\vdots\; A_{k \times (n-k)} \right]$ (n columns)

{Generator matrix of lin code always has a systematic form}

$$d \leq \text{wt(row)} \leq n - k + 1$$

Codes which achieve singleton bound: Maximum Distance Seperable code or MDS code

↳ Eg: Repetition code $(n, 1, n)$

Parity check code $(n, n-1, 2)$

Reed Solomon code: $GF(q)$, $q > n$

$\alpha_1, \alpha_2 \cdots, \alpha_n$ from $GF(q)$ {distinct}

RS code: $H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & & & \alpha_n \\ \alpha_1^2 & & & & \\ \vdots & & & & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \cdots & & \alpha_n^{n-k-1} \end{bmatrix}$ ($n-k$ rows, n columns)

$G = \begin{bmatrix} & & & \\ & & & \end{bmatrix}$ (k rows, n columns)

Claim: Min dist $= n-k+1$

Any $n-k$ columns are lin. ind. $B = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & & & \beta_{n-k} \\ \vdots & & & \vdots \\ \beta_1^{n-k-1} & & \cdots & \beta_{n-k}^{n-k-1} \end{bmatrix}$

$\det(B) = \prod_{\substack{i,j \\ 1 \le i < j \le n-k}} (\beta_i - \beta_j)$

$G \begin{cases} 1^{st}: & (1) : (n-k+1) \\ k^{th}: & k : n \end{cases}$

Gilbert Varshamov Bound

Claim 1: GF(q); (n, k, d) satisfies $q^k < \dfrac{q^n}{Vol_q(n-1, d-2)}$, where $Vol_q(n-1, d-2) = \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$

then $\exists$ (n, k, d) code

Claim 2: we can construct a lin code. s.t. $A_q(n, d) \ge \dfrac{q^n}{Vol_2(n, d-1)}$

Claim 1:

Pf: Maximal code C, $|C| = A_q(n, d)$

$x \in F_q^n$, $\exists\, c_x$ s.t. $d(x, c_x) \le d-1$

{otherwise we can add x to the code}

$q^n \le |C| \cdot Vol_q(n, d-1) \Rightarrow |C| = A_q(n, d) \ge \dfrac{q^n}{Vol_q(n, d-1)}$

Claim 2:

Pf: construct an $(n-k) \times n$ parity check matrix s.t. every set of $d-1$ columns to be lin. indep.

start with $(n-k) \times (n-k)$ identity matrix

we have selected $\ell-1$ columns already $h_1, h_2, \cdots, h_{\ell-1} \in F_q^{n-k}$

Need to find h_ℓ

h_ℓ should not lie in the span of $d-2$ columns from $h_1, \cdots, h_{\ell-1}$

(cannot be of the form) $h_\ell = [\, h_1 \; h_2 \; \cdots \; h_{\ell-1} \,] \cdot x$ where $wt(x) \le d-2$

coef vectors : $Vol_q(\ell-1, d-2)$

ineligible vectors $\le Vol_q(\ell-1, d-2)$

Space of choices of h_ℓ is q^{n-k}

As long as $q^{n-k} \ge$ # ineligible vectors

$\Rightarrow$ sufficient if $q^{n-k} \ge Vol_q(\ell-1, d-2)$

Roth Thm 4.5 $F = GF(q)$; $\delta = \frac{q^k - 1}{q-1} \cdot \frac{Vol_q(n, d-1)}{q^n}$

Then all but δ fraction of (n,k) lin codes over $GF(q)$ have min dist $\geq d$

$q = 2$, if $2V_2(n, d-1) < 2^{n-k}$, then $\geq 1/2$ of indr lin code have min dist $\geq d$

$$2^k < \frac{2^n}{2\,vol(n, d-1)}$$

Asymptotic Bounds

(n, k, d) code

$R = \frac{k}{n}$, normalized distance $\delta = \frac{d}{n}$

R & δ $\quad R, \delta > 0$

An "asymptotically good code" is a code family which has asymptotically positive normalized /rel distance $\delta > 0$

$$\lim_{n\to\infty} \frac{d}{n} > 0$$

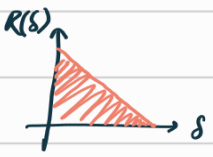
and asy. positive rate $\quad R(\delta) = \lim_{n\to\infty} \frac{\log_q(A_q(n, \delta n))}{n} > 0$

Example: Hamming Code: $\delta = \lim_{m\to\infty} \frac{3}{2^m - 1} = 0$

Singleton Bound: $A_2(n,d) \leq 2^{n-d+1}$

$$\frac{\log(A_2(n,d))}{n} \leq \frac{n-d+1}{n}$$

$$\Rightarrow \quad R(\delta) \leq 1 - \delta$$



Hamming Bound: $A_2(n,d) \leq \frac{2^n}{Vol_2(n, \lfloor \frac{d-1}{2} \rfloor)}$

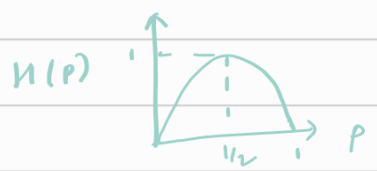
$$R(\delta) \leq \lim_{n\to\infty} \frac{n - \log Vol_2(n, \lfloor \frac{d-1}{2} \rfloor)}{n}$$

$p \leq 1/2 \qquad Vol_2(n, pn) = \sum_{i=0}^{pn} \binom{n}{i}$

$$\lim_{n\to\infty} Vol_2(n, pn) \approx 2^{n \cdot H(p)}$$

$H(p) = -p \log p - (1-p)\log(1-p)$

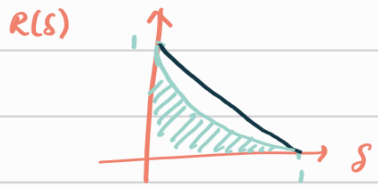
↑ entropy



$$R(\delta) \leq \lim_{n\to\infty} \frac{n - \log\left(\binom{n}{\lfloor \frac{d-1}{2} \rfloor}\right)}{n}$$

Stirling's approximation: $\frac{1}{n}\log\binom{n}{np} \to H(p)$

$$\leq 1 - H(\delta/2)$$



GV bound $\exists$ (n, m) code s.t.

$$2^k \geq \frac{2^n}{\mathrm{Vol}_2(n, d-1)}$$

$$R = \lim_{n\to\infty}\left\{\frac{k}{n} \geq \frac{n - \log_2 \mathrm{Vol}_2(n, d-1)}{n}\right\}$$

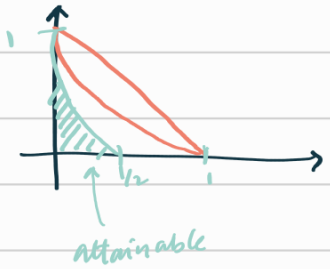
$$\mathrm{Vol}_2(n,t) \leq 2^{nH(t/n)} \quad \forall t \leq n/2$$

$$\geq \lim_{n\to\infty} \frac{n - nH\left(\frac{d-1}{n}\right)}{n}$$

$$= 1 - H(\delta)$$

$$R \geq 1 - H(\delta)$$

$$H(\delta) = -\delta\log\delta - (1-\delta)\log(1-\delta)$$



$$2^{-nH(t/n)} \cdot \mathrm{Vol}(n,t) = \left(\frac{t}{n}\right)^t \left(1 - \frac{t}{n}\right)^{n-t} \cdot \left(\sum_{i=0}^{t}\binom{n}{i}\right)$$

$$\leq (t/n)^t \left(1 - t/n\right)^{n-t} \cdot \left(\sum_{i=0}^{t}\binom{n}{i}\left(\frac{n-t}{t}\right)^{t-i}\right)$$

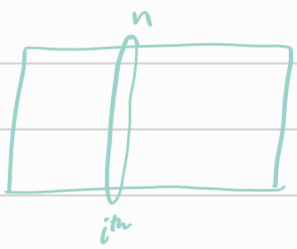
$$= \sum_{i=0}^{t}\binom{n}{i}\left(\frac{t}{n}\right)^i \left(1 - t/n\right)^{n-i} \leq 1$$

Plotkin Bound – $A_2(n,d) \leq \frac{2d}{2d-n} \quad \forall\ d \geq n/2$

For $\delta > 1/2$: $\lim_{n\to\infty} \frac{\log A_2(n,d)}{n} \leq \lim_{n\to\infty} \frac{\log \frac{2d}{2d-n}}{n} \to 0$

Positive asymptote in $\delta > 1/2$ is not possible !!

Pf:



m codewords

x_i = # of 1s in the i^{th} column

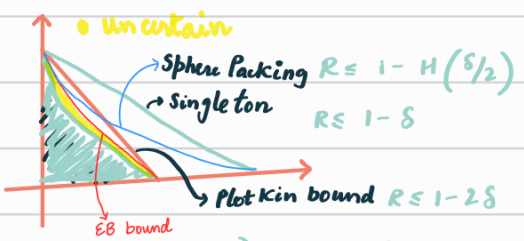
$$\sum_{i \neq j} d(c_i, c_j) = \sum_{k=1}^{n} x_k (m - x_k)$$

$$\binom{m}{2} d \leq \leq n \frac{m^2}{4}$$

$$\frac{m(m-1)}{2} d \leq n \frac{m^2}{4} \Rightarrow m \leq \frac{2d}{2d-n} \quad \{d \geq \frac{n}{2}\}$$

$R(\delta) \leq 1 - 2\delta$

Pf: $f : C \to \{0,1\}^{n-2d+1}$



$f(c_1 \cdots c_n) = (c_1 c_2 \cdots c_{n-2d+1})$ {first $n-2d+1$ bits}

$x \in \{0,1\}^{n-2d+1}$

$C_x = \{(c_{n-2d+2}, c_{n-2d+3} \cdots, c_n) : f(c) = x\}$

C_x : All strings in C_x are of length $2d-1$ and min dist. $\geq d$

Use Plotkin $|C_x| \leq \frac{2d}{2d-(2d-1)} = 2d$

$$|A_2(n,d)| \leq 2^{n-2d+1} \cdot 2d$$
$$= d \cdot 2^{n-2d+2}$$

{take log & limit}

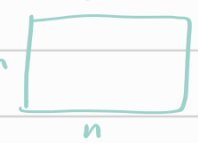
$$\Rightarrow R(\delta) \leq 1 - 2\delta$$

Elias Bassaygo Bound

$$R(\delta) \leq 1 - H\left(\frac{1 - \sqrt{1-2\delta}}{2}\right)$$

Johnson Bound: constant weight codes

$A(n, d, \omega)$



$\rightsquigarrow \binom{m}{2} d \leq \sum x_i (m - x_i)$

$\sum x_i = m\omega$

$= m^2\omega - \sum_{i=1}^{n} x_i^2$ } RMS-AM

$$\frac{m(m-1)}{2} d \leq m^2\omega - \frac{m^2\omega^2}{n}$$

$$m \leq \frac{2nd}{(n-2\omega)^2 - n(n-2d)}$$

for $\omega < \frac{n - \sqrt{n^2 - 2nd}}{2}$

Lemma: set $C \subseteq \{0,1\}^n$, $x \in \{0,1\}^n$

$$C + x = \{x + c : c \in C\}$$

$$\sum_{x \in \{0,1\}^n} |(x+C) \cap A| = |C| \cdot |A|$$

Pf:

$$= \sum_x \sum_c \sum_a \mathbb{1}_{x+c=a} = \sum_c \sum_a \sum_x \mathbb{1}_{x=a-c}$$

$$= \sum_c \sum_a 1 = |C| \cdot |A|$$

$C \to (n,k)$ code with min dist d

$A \to$ set of all n-length vectors with HW w

$(x+C) \cap A \to$ constant weight code with min dist d.

$\exists\, x$ s.t. a constant weight code with min dist d & $\geq \frac{|C|\binom{n}{w}}{2^n}$

$$|C| \leq \frac{2^n \cdot 2nd}{\binom{n}{w}\left((n-2w)^2 - n(n-2d)\right)}$$

choose w to make it 1

$$\Rightarrow |C| \leq \frac{2^n \cdot 2nd}{\binom{n}{n - \frac{\sqrt{n^2-2nd+1}}{2}}}$$

$$\lim_{n\to\infty} \frac{n - \log 2nd - \log\binom{n}{\theta n}}{n}$$

$$= 1 - H(\theta) \qquad \theta = \frac{1-\sqrt{1-2\delta}}{2}$$

MRRW state of the art asymptotic bounds

Mac William's Identities

(n, k) binary lin. code

Weight dist $= \{A_0, A_1, \dots A_n\}$

Weight enumeration polynomial $A(z) = A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n$

$C^\perp$ $\bar{B} = (B_0, B_1, B_2 \cdots, B_n)$

$B(z) = B_0 + B_1 z + B_2 z^2 + \cdots + B_n z^n$

Relationship between $A(z)$ & $B(z)$ $\quad B(z) = \frac{1}{2^k} \sum_{i=0}^{n} A_i (1-z)^i (1+z)^{n-i}$

$$= \frac{1}{2^k} (1+z)^n A\left(\frac{1-z}{1+z}\right)$$

$$B_j = \frac{1}{2^k} \sum_{i=0}^{n} A_i K_{ij}^{(n)} \qquad j = \{0, 1, \cdots, n\}$$

$$K_{ij}^{(n)} = \sum_{h=0}^{i} (-1)^h \binom{i}{h} \binom{n-i}{j-h}$$

Parity check code: (3,2) $\quad (n=3, k=2)$ $\quad \bar{A} = (1\ 0\ 3)$

$$A(z) = 3z^2 + 1$$

$$\Rightarrow B(z) = \frac{1}{4}(1+z)^3 \left(1 + 3\left(\frac{1-z}{1+z}\right)^2\right)$$

$$= 1 + z^3$$

$B = [1\ 0\ 0\ 1]$ ← (3,1) repitition code

Pf: $x = (x_1, x_2, \cdots, x_n)$

$|x| = HW(x)$

$f(x,y) = (-1)^{\langle x,y \rangle}$

$\langle x,y \rangle = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n$

$f(010, 111) = (-1)^{\langle \cdots \rangle} = -1$

$f(110, 111) = (-1)^0 = 1$

Two technical lemmas will be needed

Lemma 1 - (n,k) linear code C, $y \in \{0,1\}^n$

$$\sum_{x \in C} f(x,y) = \begin{cases} 2^k & \text{if } y \in C^\perp \\ 0 & \text{o.w.} \end{cases}$$

Pf: From def: 2^k

$y \notin C^\perp \Rightarrow \exists\, x_0 \in C \quad \langle x_0 | y \rangle \neq 0$

$\Rightarrow f(x_0, y) = -1$

For any $x \in C$, if we have $f(x,y) = 1$

$\Rightarrow f(x + x_0, y) = -1$

Lemma 2 — $x \in \{0,1\}^n$, $|x| = i$

V_j denote all vectors in $\{0,1\}^n$ with weight j

$$\sum_{y \in V_j} f(x,y) = K_{ij}^{(n)}$$

$$= \sum_{h=0}^{j} (-1)^h \binom{i}{h} \binom{n-i}{j-h}$$

Pf: $x = (\underbrace{1111}_{i}\ \underbrace{000}_{n-i}\ 0)$

vectors $y \in V_j$, which share h ones with x.

$= \binom{i}{h}\binom{n-i}{j-h}$

for each y, $f(x,y) = (-1)^h$

$$\sum_{y\in V_j}\sum_{x\in C} f(x,y) = \sum_{x\in C}\sum_{y\in V_j} f(x,y)$$

$$\sum_{y\in V_j\cap C^\perp} 2^k = B_j \cdot 2^k$$

$$= \sum_{i=0}^{n} A_i K_{ij}^{(n)}$$

Some applications of MWs

① Prob. of undetected errors over BSC

$$P_u(\varepsilon) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$

$$= (1-p)^n \left(A\left(\frac{p}{1-p}\right) - 1 \right)$$

$$B(1-2p) = \frac{1}{2^k}(2-2p)^n A\left(\frac{p}{1-p}\right)$$

$$= 2^{-(n-k)} B(1-2p) - (1-p)^n$$

Example:

$(7,4)$ HC : $H = \begin{bmatrix} 0&0&0&1&0&1&1 \\ 0&1&0&1&1&0&1 \\ 1&0&0&0&1&1&1 \end{bmatrix}$

$C^\perp = \{$
0000000
0010111
0101101
0111010
1000111
1011010
1101100
1110001
$\}$

$B(z) = 1 + 7z^4$

$P_u(\varepsilon) = 2^{-3}\left(1 + 7(1-2p)^4\right) - (1-p)^7$

② Probability of decoding error over BSC (p)

Suppose: transmit $\underline{0}$ codeword & use Maximum likelihood decoding

$$\hat{c} = \underset{c\in C}{\operatorname{argmax}}\ \mathbb{P}(y = r_x \mid t_x = c)$$

$$P_e = \sum_{c\in C\setminus\{0\}} \mathbb{P}(\hat{c} = c)$$

$$= \sum_{c\in C\setminus\{0\}} \sum_{y\in D(c)} \mathbb{P}(y\, r_x \mid \underline{0}\, t_x)$$

$D(c) \rightarrow$ decoding region corresponding to c

$$\leq \sum_{c \in C \setminus \{0\}} \sum_{y \in D(c)} \sqrt{P(y|0)\, P(y|c)}$$

As $P(y|0) \leq P(y|c)$

$$= \sum_{c \in C \setminus \{0\}} \sum_{y \in D(c)} \prod_{i=1}^{n} \sqrt{P(y_i|0)\, P(y_i|c_i)}$$

(summing to all possible y)

$$\leq \sum_{c \in C \setminus \{0\}} \prod_{i=1}^{n} \sum_{\omega \in \{0,1\}} \sqrt{P(\omega|0)\, P(\omega|c_i)}$$

$\pi\,(\omega=0)+(\omega=1)$

$$= \sum_{c \in C \setminus \{0\}} \prod_{j, c_j \neq 0} \sum_{\omega=0}^{1} \sqrt{P(\omega|0)\, P(\omega|1)}$$

(next product terms one!)

$$\gamma = \sum_{\omega=\gamma} \sqrt{P(\omega|0)\, P(\omega|1)}$$

output alphabet

← Bhatacharya Const. $= 2\sqrt{p(1-p)}$ $\quad \gamma_{BSC}$

$\gamma_{BSC} = p$

$$P_e \leq \sum_{c \in C \setminus \{0\}} \gamma^{d(c,0)}$$

$$= \sum_{\omega=1}^{n} A_\omega \gamma^\omega = A(\gamma) - A_0 = A(\gamma) - 1$$

③ Bounds on code parameters

$$B_j = \frac{1}{2^k} \sum_{i=0}^{n} A_i K_{ij}^{(n)}$$

n, k, d code

$A_0 = 1$

$A_1, A_2 \cdots, A_{d-1} = 0$

$K_{0j}^{(n)} = \binom{n}{j}$

↳ z^i in $(1+z)^n$

$j \in \{0,1,\cdots j\} \leftarrow \sum A_i K_{ij}^{(n)} \geq -\binom{n}{j}$

$$\max \; 1 + \sum_{i=d}^{n} \omega_i$$

s.t. $\omega_i \geq 0$, $d \leq i \leq n$

$$\forall j \in \{0,1,\cdots,n\} \quad \sum \omega_i K_{ij}^{(n)} \geq -\binom{n}{j}$$

Stochastic Channel

Encoder $\{0,1\}^k \longrightarrow \{0,1\}^n$

Decoder $\{0,1\}^n \longrightarrow \{0,1\}^k$

$Pr(\text{Error}) = Pr(Dec(Enc(x)) \neq x) \xrightarrow[n\to\infty]{} 0$ Vanishing Error Prob

Find the largest possible rate from Shannon (1948)

Capacity $C \rightarrow$ Max Rate

For $\forall R < C$, rate R is attainable with vanishing error rate

$R > C$, doesnot exist.

For BSC: $C = 1 - H(p) \sim -p\log p - (1-p)\log(1-p)$

BEC $C = 1-p$

Part①: $R > C$ is not possible: $c \; t_x$, $y \; r_x$

$y = c + e$

$C \rightsquigarrow$ has k bit of information

$\binom{n}{np} \sim 2^{nH(p)}$ → Cardinality of Set with high probability error patterns

$$Pr\left(\begin{array}{l}\text{Err vector}\\ \#1\}np\\ \#0\}n(1-p)\end{array}\right) = p^{np}(1-p)^{n(1-p)} \sim 2^{-nH(p)}$$

k bits of information $\;\&\;$ $nH(p)$ bits of information about the error vector.

$n > k + nH(p)$

$\Rightarrow R \leq 1 - H(p)$

with adversarial the min distance should be $2np$.

$\rightsquigarrow$ GV bound $R \approx 1 - H(2p)$

Achievability:

Generator matrix G

$\{Pr(G \text{ is full rank}) \to 1 \text{ as } n \to \infty\}$

each entry $\sim Ber(1/2)$

$\{u \in \{0,1\}^k \rightarrow uG$ is a random codeword $(uG)_i \sim Ber(1/2)$

$u \neq \{0\,0\cdots 0\}$

MLD : Bhattacharyya bound

$$P_e \le \sum_{c \in C \setminus \{0\}} \gamma^{d(c,0)}$$

$$= \sum_{\omega=1}^{n} A_\omega \left(2\sqrt{p(1-p)}\right)^\omega$$

$$\bar{P}_e \le \sum_{\omega=1}^{n} E[A_\omega] \left(2\sqrt{p(1-p)}\right)^\omega$$

$$E(A_\omega) = \sum_{\substack{u \in \{0,1\}^k \\ u \neq \bar{0}}} Pr(wt(uG) = \omega)$$

$$= (2^k - 1) \frac{\binom{n}{\omega}}{2^n}$$

$$\approx \binom{n}{\omega} 2^{k-n}$$

$$\bar{P}_e \le \sum_{\omega=1}^{n} E(A_\omega) \left(2\sqrt{p(1-p)}\right)^\omega$$

$$= \sum_{\omega=1}^{n} \frac{\binom{n}{\omega}}{2^{n-k}} \left(2\sqrt{p(1-p)}\right)^\omega \le \frac{1}{2^{n-k}} \left(1 + 2\sqrt{p(1-p)}\right)^n$$

$$\bar{P}_e \le 2^{n[R - 1 + \log(2p\sqrt{1-p})]}$$

$\downarrow 0$ as $n \to \infty$ if $R < 1 - \log(2p\sqrt{1-p})$

not tight enough bound to get a tighter bound.

We now try to obtain a better bound:

Decoding rule is updated: Q_{tx}

If $\exists!\ c \in C$ s.t. $(d(y,c) - np) \le \varepsilon n$, $\varepsilon > 0$ is small

then output c.

Otherwise error.

Error events:

① $|wt(y) - np| > \varepsilon n$

② $\exists$ a codeword other than $\bar{0}$ s.t. $|d(y,c) - np| \le \varepsilon n$

$$P_e \le P(|wt(y) - np| > \varepsilon n) + P(\exists\ c \in C \setminus \{0\},\ |d(y,c) - np| \le \varepsilon n,\ |wt(y) - np| \le \varepsilon n)$$

Hoeffding's $2^{-np\varepsilon^2}$

$$\le \sum_{\omega=1}^{n} A_\omega P\left(wt(y) \approx np,\ d(y,c) \approx np \mid wt(c) = \omega\right)$$

$$\leq \sum_{w=1}^{n} A_w \cdot \frac{\binom{w}{w/2}\binom{n-w}{np-w/2}}{\binom{n}{np}}$$

$\downarrow \varepsilon(A_w)$

$$\leq \sum_{w=1}^{n} \frac{\binom{n}{w}}{2^{n-k}} \frac{\binom{w}{w/2}\binom{n-w}{np-w/2}}{\binom{n}{np}}$$

$$\leq \frac{n\binom{n}{np}}{2^{n-k}}$$

$$\leq n \cdot 2^{n[R-1+H(p)]}$$

$\downarrow n \to \infty \quad R < 1 - H(p)$

BEC & Bhatacharya bound:

$$\bar{P}_e \leq 2^{n[R-1+\log(1+r_{BEC})]}$$

$$= 2^{n[R-1+\log(1+p)]}$$

$$R < 1 - \log(1+p)$$

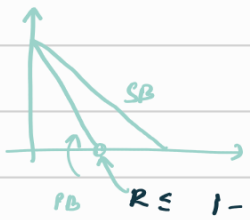
Decoding → 'Joint typicality'

↳ Declare o/p to be C if it agrees with y in all non erased locations

Maximal Distance Seperable

Singleton Bound

$d \le n-k+1$



Reed Solomon Code

$q > n$, RS code is MDS

C [ ] $G = k$ [|] n (k, n-k) $H = n-k$ [|] n (n, n-k) ✓

$d = n-k+1$, $d \ge 1$

MDS conjecture: For almost all k, a k-dim code is MDS only if $n \le q+1$

MDS code needs $q \ge n-d+2$

Pf: MDS code (n,k) $d = n-k+1$. Puncture at $(d-3)$ positions

↳ Resulting code $(n-d+3, k, =3)$ { Puncturing $\Rightarrow \ge 3$, Singleton $\Rightarrow \le 3$ } $\Rightarrow = 3$

Sphere packing: $q^{n-d+1} \le \frac{q^{n-d+3}}{1+(q-1)(n-d+3)}$

$\Downarrow$

$q \ge n-d+2$

Reed Solomon Code

Polynomials over $\mathbb{F}_q$ $f(x) = a_0 + a_1 x + a_2 x^2 \cdots + a_d x^d$ $\in \mathbb{F}_q$

Properties:

→ $f(x)$ with degree d over $\mathbb{F}_q$ has atmost d roots.

$(x-r_1) \mid f(x)$

$\vdots$

$(x-r_d) \mid f(x)$ $\Rightarrow$ $d+1$ polynomial $\mid f(x)$ ↗ contradiction

Ex $\mathbb{F}_3$ $f(x) = x^2-1 \to \{0,2\}$ (roots) (Evaluating the function)

	0	1	2
	1	2	2

$f(x) = x^2+1 \to \emptyset$

	0	1	2
	1	1	0

$f(x) = x^2+2x+1 \to \{2\}$

→ 'Interpolation' Given $\{(x_i, y_i)\}_{i=1}^{d+1}$ $\{$distinct $x_i\}$ s.t. $f(x_i) = y_i$

$\Rightarrow$ ∃! polynomial f with degree $\le d$ over $\mathbb{F}_q$

s.t. $f(x_i) = y_i$

Pf: $f(x) = a_0 + a_1 x + \cdots + a_d x^d$

$\bar{x}\ a = y$

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^d \\ 1 & x_2 & \cdots & & x_2^d \\ \vdots & & & & \\ 1 & \cdots & & & x_{d+1}^d \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d+1} \end{bmatrix}$$

Full rank matrix $\Rightarrow$ $a = \bar{x}^{-1} y$

Vandermonde matrix

Lagrange Interpolation

$$p(x) = \sum_{i=1}^{d+1} f(x_i) \cdot l_i(x)$$

$$l_i(x) = \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)} \qquad \begin{cases} 0 & \text{for } x = x_j\ \forall j \neq i \\ 1 & \text{for } x = x_i \end{cases}$$

Polynomial Interpretation of RS codes

$q > n \geq k$ RS code

for evaluation pts $\bar{r} = (r_1, r_2, \cdots r_n)$ taking non zero pts.

$$RS(\bar{r}, n, k) = \left\{ (f(r_1), f(r_2), \cdots, f(r_n)) : f(x) \in \mathbb{F}_q[x],\ \deg(f) \leq k-1 \right\}$$

q^k polynomials

Message is polynomial

Message bits $\{u_0, u_1, \cdots, u_{k-1}\}$ $f_u(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_{k-1} x^{k-1}$

Evaluated at $\bar{r}$

Code word $(f(r_1), f(r_2), \cdots, f(r_n))$

Same at max $k-1$ positions

$\Rightarrow d \geq n - (k-1) = n-k+1$

Claim: $RS(\bar{r}, n, k)$ is MDS

$d = n-k+1$

no. of zeros is $\leq k-1 \Rightarrow$ non zero entries $\geq n-k+1$

Generator matrix:

$$[u_0\ u_1\ \cdots\ u_{k-1}] \underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_n \\ \vdots & & & \vdots \\ r_1^{k-1} & & & r_n^{k-1} \end{bmatrix}}_{G} = c$$

Even if we get just k code bits, we can reconstruct the message bits.

→ Dual of MDS is also an MDS code.

Dual View

$\mathbb{F}_q$, $\mathbb{F}_q^*$ → multiplicative groups consisting of all nonzero elements from $\mathbb{F}_q$.

$\mathbb{F}_3$, $\mathbb{F}_3^* = \{1, 2\}$ under mod 3 multiplication

Fact: $\mathbb{F}_q^*$ is cyclic, i.e., $\exists\ \alpha \in \mathbb{F}_q^*$ which generates $\mathbb{F}_q^*$

$\alpha^{q-1} = 1$

$\langle 1 \rangle = \{1\}$ $\quad\quad$ $\langle 4 \rangle = \{1, 4\}$

$\langle 2 \rangle = \langle 3 \rangle = \{1, 2, 3, 4\}$

Fact 2: For any $0 < \ell < q-1$ $\quad\quad$ $\sum_{r \in \mathbb{F}_q} r^\ell = 0$

Pf:

$$\sum r^\ell = \sum_{j=0}^{q-2} \alpha^{j\ell} = \frac{1 - (\alpha^\ell)^{q-1}}{1 - \alpha^\ell}$$

$\alpha^{q-1} = 1$

α is called a primitive element of $\mathbb{F}_q$

$\bar{\alpha} = \{\alpha^0, \alpha^1, \cdots, \alpha^{n-1}\}$

$RS(\bar{\alpha}, n, k) = \{ (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{F}_q^n$ s.t. $C(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ & $C(\alpha^j) \neq 0$ $\forall\ j \in 1, 2, \cdots, d-1 = n-k \}$

$$\underbrace{\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & & & & \\ 1 & \alpha^{n-k} & (\alpha^{n-k})^2 & \cdots & (\alpha^{n-k})^{n-1} \end{bmatrix}}_{(n-k) \times n} \underbrace{\begin{bmatrix} c_0 \\ \vdots \\ c_n \end{bmatrix}}_{n \times 1} = \begin{bmatrix} \vdots \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

$$G = \underbrace{\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & & \alpha^{n-1} \\ \vdots & \alpha^2 & (\alpha^2)^2 & & \\ 1 & & & & (\alpha^{n-1})^{k-1} \end{bmatrix}}_{K \times n}$$

Review in moodle notes.

Decoding of Reed Solomon Codes

Berle kamp - Massay order $(n \log n)$

Berle kamp - Welch - order (n^3)

Decode $RS(\mathbb{F}, n, K)$ upto e errors

$$e \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{n-K}{2} \right\rfloor$$

$r = (r_1, \ldots, r_n)$

Find a polynomial $f \in \mathbb{F}_q[x]$

① $\deg(f) \leq k-1$ ② $f(r_i) \neq r_i$ in atmost e locations

Idea : Error locator polynomial

$$E(x) = \prod_{i : r_i \neq f(r_i)} (x - r_i) \qquad \deg(E(x)) \leq e$$

↑ Dont know it before decoding.

But : $\forall i$, $r_i E(r_i) = \underbrace{f(r_i) E(r_i)}_{Q(r_i)}$

Find $E(x)$, $Q(x)$, $\hat{f}(x) = \frac{Q(x)}{E(x)}$

① Find:

(a) Monic Polynomial $E(x)$ with degree e.

(b) a polynomial $Q(x)$ of degree $\leq e+k-1$

s.t. $r_i E(r_i) = Q(r_i) \quad \forall i$

If unable to find E, Q, then declare error

② $\hat{f}(x) = \frac{Q(x)}{E(x)}$

If $\hat{f}(r_i) \neq r_i$ at more than e locations, declare error o.w. o/p $\hat{f}$

Ⓐ How do we know that we will find some E, Q ?

Ⓑ How do we know that we will get a consitent $\hat{f}$.

Claim 1: If $\exists\ f$ with $\deg(f) \le k-1$ s.t. $f(r_i)$ & r_i different in $\le e$ locations, then $\exists\ E$ & Q that satisfy

Existence

Pf: $E(x) = \prod_{i : f(r_i) \neq r_i} (x - r_i) \cdot x^{e - \Delta_{fr}}$

↑ degree $= e$

↖ Δ_{fr} is the no. of places where $f(r_i)$ & r_i differ

$Q(x) = E(x) \cdot f(x)$

Claim 2: If (Q_1, E_1) & (Q_2, E_2) satisfy (*), then $\frac{Q_1}{E_1} = \frac{Q_2}{E_2}$

Constiency

Pf: $R(x) = \underbrace{Q_1(x)}_{e+k-1}\ \underbrace{E_2(x)}_{e} - Q_2(x) E(x)$

$\deg R(x) \le 2e + k - 1 = 2\left\lfloor \frac{n-k}{2} \right\rfloor + k - 1 < n$

$\forall\ i,\ R(r_i) = Q_1(r_i) E_2(r_i) - Q_2(r_i) E_1(r_i)$

$= r_i E_1(r_i) E_2(r_i) - r_i E_2(r_i) E_1(r_i)$

$= 0$

↖ n roots, degree $< n$

$\Rightarrow R(x)$ is 0.

Example: $q = 7,\ n = 5,\ k = 3;\ d = 3,\ e \le 1$

RS $(\bar{F}(1,2,3,4,5); 5; 3)$, $u = (u_0, u_1, u_3) = (1\ 1)$

$f_u = 1 + x + x^2$

Sent Codeword : $(3, 0, 6, 0, 3)$

↓ channel

Received word : $(3, 1, 6, 0, 3)$

$E(x)$, $Q(x)$

↑ ↑

$x + b_0$ $\quad a_0 + a_1 x + a_2 x^2 + a_3 x^3$

$1 \rightarrow \quad 3(1 + b_0) = (a_0 + a_1 + a_2 + a_3)$

$2 \rightarrow \quad 1(2 + b_0) = (a_0 + 2a_1 + 4a_2 + a_3)$

$3 \rightarrow \quad 6(3 + b_0) = (a_0 + 3a_1 + 2a_2 + 6a_3)$

$4 \rightarrow \quad 0(4 + b_0) = (a_0 + 4a_1 + 2a_2 + a_3)$

$5 \rightarrow \quad 3(5 + b_0) = (\ \ldots\ )$

Upon solving : $a_3 = 1,\ a_2 = 6,\ a_1 = 6,\ a_0 = 5,\ b_0 = 5$

$$E(x) = x+5$$

$$Q(x) = 5 + 6x + 6x^2 + x^3$$

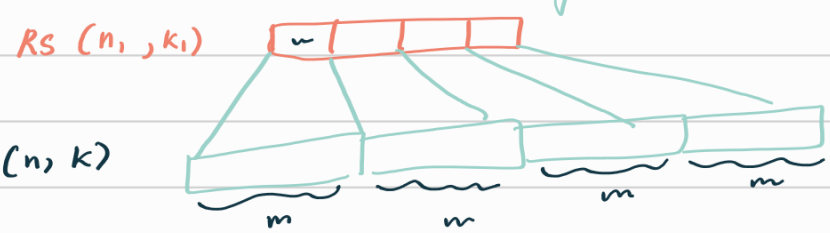
$$\Rightarrow \hat{f}(x) = x^2+x+1$$

we dont know if $E(x) \mid Q(x)$ when there are more than $\frac{\delta}{2}$ errors & we are able to find such $E(x), Q(x)$ in step 1.

Binary form of RS code

$q = 2^m$ $\quad (n_1, k_1)$ RS code over $\mathbb{F}_q$ $\quad q > n$

$\hookrightarrow (n, k)$ binary code



$$n = n_1 \log_2 q = n_1 m$$

$$k = k_1 \log_2 q = k_1 m$$

$$d \geq n_1 - k_1 + 1$$

Rate is same !!

$$\delta \geq \lim_{n_1 \to \infty} \frac{n_1 - k_1 + 1}{n_1 \log_2 q} = \lim_{n_1 \to \infty} \frac{1 - R}{\log_2 q} = 0$$

Another way : Bose Roy Chaudhuri & Hoq...

$$BCH \longrightarrow RS_q(n,k) \cap \{0,1\}^n$$

$q = 2^m$, $n = 2^m - 1$, α is a primitive element

$$BCH = \left\{ (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_2^n : \; C(\alpha^j) = 0 \quad \forall j = 1, 2, \dots, d-1 \right\}$$

$$C(x) = \sum_{i=0}^{n-1} c_i x^i$$

Min distance $\geq d = n - k + 1$

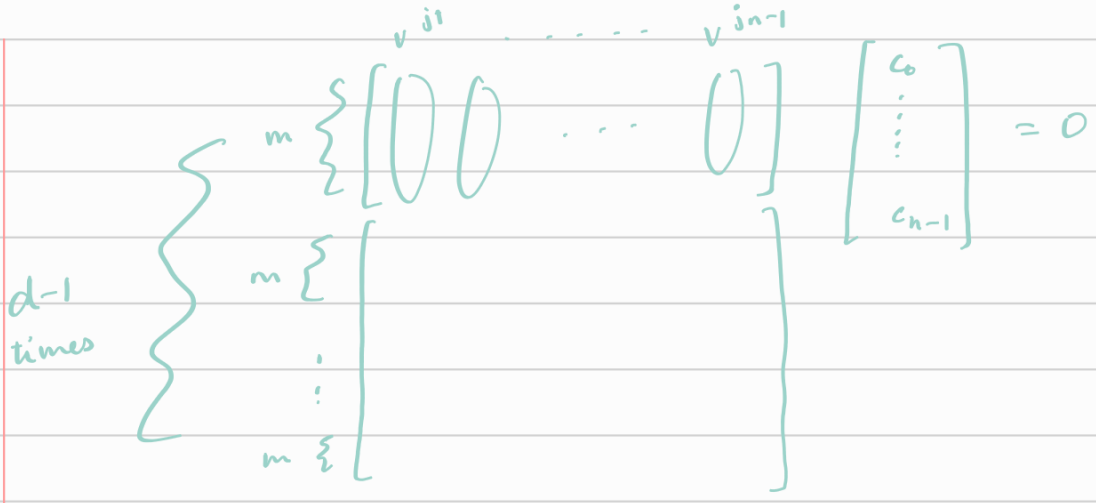
Prop: BCH code over $\mathbb{F}_q$ - code with min. distance $\geq d$ & $k \geq n - (d-1)\log(n+1)$

Pf: $(c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_2^n$, $C(x) = \sum_{i=0}^{n-1} c_i x^i$

, $C(\alpha^i) = 0 \quad \forall i \in \{1, 2, \dots, d-1\}$

$\alpha^j = (a_1, a_2, \dots, a_m) \rightarrow$ binary vector of length m

$$\sum_{i=0}^{n-1} c_i \cdot (\alpha^{ij}) = 0 \qquad \sum_{i=0}^{n-1} c_i \, v^{ji} = 0$$



$m \cdot (d-1)$ constraints

Dim code $\geq n - m(d-1)$

$= n - (d-1)\log(n+1)$

$d-1 \geq \frac{n-k}{\log(n+1)} \rightsquigarrow \delta \geq \frac{1-R}{\log n}$ Someway $\frac{2(1-R)}{\log n}$ ← By the fact that $C(\alpha)=0 \Leftrightarrow C(\alpha^4)=0$ leads to halfing of the

Multivariate Polynomials

$$C(r,m) = \left\{ \underbrace{f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_{2^m})}_{n=2^m} \;\middle|\; f \in \mathbb{F}_2[x_1, x_2, \cdots, x_m],\ deg(f) \leq r \right\}$$

$f(x) = 1 + x_1 x_2$ → degree = 2

$$f(x) = \sum_{\substack{S \subseteq \{1,2,\cdots,m\} \\ |S| \leq r}} c_S \prod_{i \in S} x_i$$

$f(00) = 1$
$f(01) = 1$
$f(10) = 1$
$f(11) = 0$

$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$

$= Vol_2(r, m)$

Schwartz Zippel Lemma

↳ $f \in \mathbb{F}_2(x_1, x_2 \cdots x_m) \neq 0$, $deg(f) \leq r$

Non roots $= \left(\sum_{\alpha \in \mathbb{F}_2^m} \mathbb{I}(f(\alpha) \neq 0) \right) \geq 2^{m-r}$

$f(x) = \tilde{\prod_{i=1}} x_i$ has 2^{m-r} non-roots

⇒ $d = 2^{m-r}$ → Least hamming weight

This is the Reed-Muller code!!

$(r_0, r_1, \cdots, r_{2^m-1})$ differ from $(f(\alpha_0), f(\alpha_1), \cdots, f(\alpha_{2^m-1}))$ in atmost $\left\lfloor \frac{d-1}{2} \right\rfloor$ locations $(2^{m-r-1}-1)$

Lemmas before decoding strategy:

$$R_S(x) = \prod_{i \in S} x_i \qquad f(x) = \sum c_S R_S(x)$$

Lemma 1: For any set S

$$\sum_{a \in \mathbb{F}_2^{(|S|)}} R_S(a) = 1$$

only for when $\forall x_i = 1$.

Lemma 2: For any S, $T \subset S$

$$\sum_{a \in \mathbb{F}_2^{|S|}} R_T(a) = 0 \quad , i \in S \setminus T$$

$$= \sum R_T(a) + \sum R_T(a)$$

$\longrightarrow S, \ |S| = r, \ b \in \mathbb{F}_2^{m-r}$

$$\sum_{\substack{a \in \mathbb{F}_2^{|S|} \\ a_{\bar{S}} = b}} f(a) = c_S$$

$a \in \mathbb{F}_2^m, \ a_S = b$

$$\sum f_b(a) = c_S + 0$$

$$f_b(x) = c_S R_S(x) + \sum_{T \subset S} a_T R_T(x)$$

s'

$$\prod_{i \in s' \cap S} x_i \cdot c_{S'} \; R_{S \cap S'}$$

Each involves 2^r assignments # 2^{m-r} such equations

EXAMPLE:

$C(1,3)$ $\qquad f(x) = 1 + x_1 + x_2$

$x_1x_2x_3$	codeword	error		
$f(000)$ =	1	$\longrightarrow$ 0	$f(100)$ =	0
$f(001)$ =	1		$f(101)$ =	0
$f(010)$ =	0		$f(110)$ =	1
$f(011)$ =	0		$f(111)$ =	1

$S = \{1\} \rightarrow (x_2, x_3) = 11 \rightarrow (x_2, x_3) = 10$

$f(011) + f(111) = 1$; $f(110) + f(010) = 1$

Calculate: 2^{m-r} parity checks corresponding to S using received bits, use majority as estimate for c_S.

↳ $r(000) + r(100) = 0$ $\quad$ $r(010) + r(110) = 1$

$r(001) + r(101) = 1$ $\quad$ $r(011) + r(111) = 1$

Majority decoding = 1 //

$$f'(x) = f(x) - \sum_{|S|=r} \hat{c_S} \cdot \prod_{i} x_i$$

↖ Reduce the degree and iterate over the lower degree polynomial

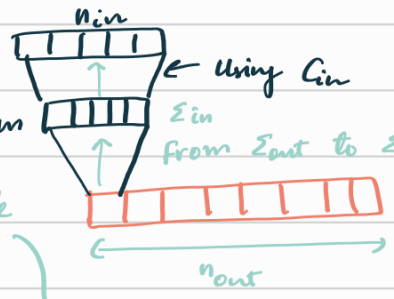
---

Concatenated code

Outer Code, Inner Code

$(n_{out}, k_{out}, d_{out})$ over Σ_{out}

(n_{in}, k_{in}, d_{in}) code over Σ_{in}



$|\Sigma_{in}|^{k_{in}} = |\Sigma_{out}|$

overall code over Σ_{in}: $\left(n_{in} \cdot n_{out},\ k_{out} \cdot k_{in},\ \geq d_{in} \cdot d_{out}\right)$

$R = \frac{k_{in} \cdot k_{out}}{n_{in} \cdot n_{out}}$

Example code: RS code: over $GF(2^3)$ (Σ_{out})

Outer Code → $n_{out} = 6$, $k_{out} = 2$ $\quad$ $RS(\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}, 6, 2)$

↑ $d_{out} = 5$ //

$u_0, u_1 \in GF(2^3)$

↳ $f_u(x) = u_0 + u_1 x$

$(f_u(\alpha), f_u(\alpha^2), \dots f(\alpha^6))$

Inner Code → Simplex code $(7, 3, 4)$ ← Dual of Hamming Code. all codewords are of same weight of 4.

n_{in} k_{in} d_{in}

$$[f_u'(\alpha), f_u^2(\alpha), f_u^3(\alpha)] \begin{bmatrix} H_{Hamming} \end{bmatrix}$$

$[\overbrace{\quad}^{7}]$ $[\overbrace{\quad}^{7}]$ $\dots$ $[\overbrace{\quad}^{7}]$

$f_u(\alpha)$ $\quad$ $f_u(\alpha^2)$ $\quad$ $f_u(\alpha^6)$

$n_{tot} = 42$, $\quad k_{tot} = 6$, $\quad d_{out} = 20$

Theorem: $d \geq d_{in} \cdot d_{out}$; $\delta \geq \delta_{in} \cdot \delta_{out}$

Proof: Take $C \neq C'$

Outer code will differ in $\geq d_{out}$ locations

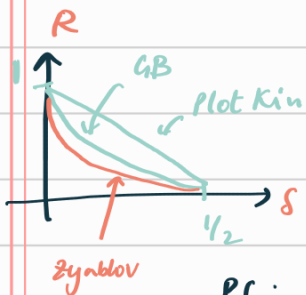
Each such location, when fed into inner code, o/p will differ $\geq d_{in}$ locations.

RS code as outer code. $\circ$ Asymp. Good Binary code as inner code $=$ Asymp. Good Binary code

Zyablov Bound

(Binary Codes)

For any $\varepsilon > 0$, there exists a family of codes which are binary & Explicit, with a symbol rate R & distance δ.



$$R \geq \sup_{r \in (0,\, 1-H(\delta)-\varepsilon)} r\left(1 - \frac{\delta}{H^{-1}(1-r-\varepsilon)}\right)$$

Pf: Via concatenate code

$C_{out} \to$ RS code with rate R_{out}, $\delta_{out} = 1 - R_{out}$

$C_{in} \to$ Binary l.h. code which lies on the GV curve $r \geq 1 - H(\delta_{in}) - \varepsilon$

- Larger r will make δ_{in} small.

we dont want δ_{in} to be smaller than δ. Hence r has an upper bound.

$$\delta \geq \delta_{in}\,\delta_{out} \geq (1 - R_{out})\, H^{-1}(1-r-\varepsilon)$$

$$R = \frac{R_{in} \cdot R_{out}}{r} \geq r \cdot \left(1 - \frac{\delta}{H^{-1}(1-r-\varepsilon)}\right)$$

RS code: $q = 2^{k_{in}}$

Eval pts $\to$ $\mathbb{F}_q^* = q - 1 = n_{out} = 2^{k_{in}} - 1$

$$k_{in} = \log q \approx \log(n_{out})$$

$$n_{in} = \frac{k_{in}}{r} = \frac{\log(n_{out})}{r} \leq \frac{\log n}{r}$$

Go over all possible $k_{in} \times n_{in}$ generator matrices

$$2^{k_{in} \times n_{in}} \leq 2^{\log^2 n / r} \leq n^{O(\log n)}$$

Enumerate all possible binary vectors of length $n_{in} \cdot K_{in}$

complexity in each phase $\rightarrow$ $2^{n_{in} \cdot K_{in}} \leq 2^{O(\log n)} \leq n^c$

Justesen Code

① Dont have to use same inner code $\forall$ outer code symbols

② Suffices to show that atleast some $(1-\varepsilon)$ fraction of inner code is good.

Outer code is R.S. $(\mathbb{F}_q^*, n_{out}, K_{out})$ $\quad R_{out} = \frac{K_{out}}{n_{out}}$

$q = 2^{K_{in}}$

$n_{out} = q-1$

Each element of outer code: $(\omega_1, \omega_2, \cdots, \omega_{n_{out}})$

will map with rate $= 1/2$ {of inner code}

$n_{in} = 2K_{in}$

$$C = \left\{ C_{in}^1(f(\alpha_1)) \cdot C_{in}^2(f(\alpha_2)) \cdots C_{in}^{n_{out}}(f(\alpha_{n_{out}})) : f \in \mathbb{F}_q[x],\ \deg(f) \leq K_{out} \right\}$$

Assume that $(1-\varepsilon)$ (very small) fraction of inner codes satisfy GV bound $\quad \delta_i \geq H^{-1}(1/2 - \varepsilon)$

Proposition: For $R_{out} \in (0,1)$, Justesen code is asymptotically good with rate $= \frac{R_{out}}{2}$.

Proof: Need to show (+ve) minimum distance in limit.

Min weight of a non zero codeword of outer symbols.

Outer code: atleast $\frac{n_{out} - K_{out} + 1}{n_{out}}$ fraction will be non zero

$\approx 1 - R_{out}$

Choose ε s.t. $1 - R_{out} > 2\varepsilon > 0$

$\rightsquigarrow$ Atmost ε of inner are bad

$\rightarrow$ At least ε fraction will non zero symbols which will be mapped via good code. $\geq H^{-1}(1/2 - \varepsilon)$

$\Rightarrow \quad d \geq (\varepsilon \cdot n_{out}) \cdot (2K_{in} \cdot \delta_i)$

Lower bound on relative distance $\delta \geq \varepsilon \cdot H^{-1}(1/2 - \varepsilon) > 0$

$\delta \geq H^{-1}(1-R-\varepsilon)$

Wozencraft Ensemble From GV, $\exists$ $\left(R \geq 1 - H(\delta) - \varepsilon \rightarrow H(\delta) \geq 1 - \frac{R}{\varepsilon}\right)$

Claim: $\varepsilon > 0$, k large enough $\exists$ a family of $(2k, k)$ codes

$C_{in}^1, C_{in}^2 \cdots C_{in}^N$ $\quad N = 2^k - 1$

s.t. for $\geq (1-\varepsilon)N$ of these C_{in} has a rel. dist. of $\geq H^{-1}(\frac{1}{2} - \varepsilon)$

Outer code - $RS(\mathbb{F}_q^*, n_{out}, k_{out})$

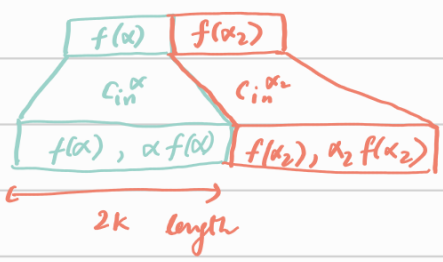
$\mathbb{F}_q$ $\quad N = q - 1$, $q = 2^k$

$(= n_{out})$

$C_{in}^{\alpha} : \mathbb{F}_2^k \longrightarrow \mathbb{F}_2^{2k}$

$C_{in}^{\alpha}(x) = (x, \alpha x)$

RS codeword each symbol is an evaluation $f(\alpha)$, $\alpha \in \mathbb{F}_q^*$



Claim: $C_{in}^{\alpha_1}$, $C_{in}^{\alpha_2}$ for $\alpha_1 \neq \alpha_2$, do not share any codeword.

Pf: Assume $y \in C_{in}^{\alpha_1}$ & $y \in C_{in}^{\alpha_2}$

$\Rightarrow$ $y = (y_1, \alpha_1 y_1)$

$y = (y_2, \alpha_2 y_2)$

$\Rightarrow \alpha_1 = \alpha_2$ $\Rightarrow$ contradiction.

{ # bad of codes in this family is bounded by

$2k$-length vector with HW $\leq 2k \cdot H^{-1}(1/2 - \varepsilon)$

As no common codeword, the no. of vectors with HW $\leq 2k \cdot H^{-1}(1/2-\varepsilon)$ can be assumed to be each in a different family.

$y \in \mathbb{F}_2^{2k}$, $wt(y) \leq 2k \cdot H^{-1}(1/2 - \varepsilon)$

$\leq Vol\,(2k, H^{-1}(\frac{1}{2} - \varepsilon)\,2k)$

$\leq 2^{2k \cdot H(H^{-1}(1/2-\varepsilon))} = 2^{k - 2k\varepsilon} \leq \varepsilon(2^k - 1) = \varepsilon N$

for large enough k

Inner Code family

$R \in (0,1)$

$r \in (1/2, 1)$

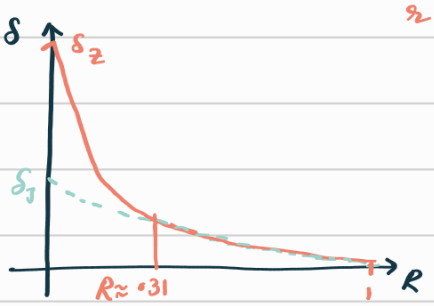
$C_{in}^{\alpha} = (x, (\alpha x)_\ell) = \frac{k}{k+\ell}$

for $R \in (0,1)$

Justesen code: $\exists$ explicit binary linear code of rate $\geq R$

& $\delta \geq \max_{r \geq \max(1/2, R)} \left(1 - \frac{R}{r}\right) H^{-1}(1-r-\varepsilon)$

↑ Additional constraint, which allows for EXPLICIT CONSTRUCTION.

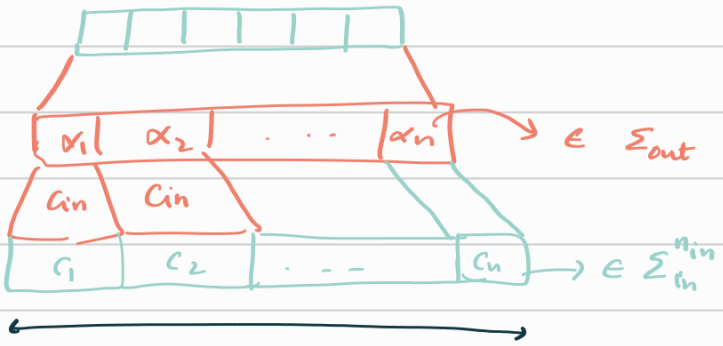


Zyablov: $\delta_2 \geq \max_{r \geq R} \left(1 - \frac{R}{r}\right) H^{-1}(1-r-\varepsilon)$

Decoding of concatenated codes

$x \in \Sigma_{in}^{k_{in} \times k_{out}} = \Sigma_{out}^{k_{out}}$

$e < \frac{d_{in} d_{out}}{2} - 1$



$y_i \rightarrow$ the i^{th} recieved word

1st Attempt: ① Decode each of the inner code blocks: $\hat{c}_i$ closest to y_i $\in C_{in}$

② Use C_{in}^{-1} to convert $\hat{c}_i$ to $\hat{\alpha}_i \in \Sigma_{out}$

③ Decode C_{out} to get original message

Call an output block bad if # errors is $\geq \lfloor \frac{d_{in}-1}{2} \rfloor$

Total no of errors is e then

bad blocks $\leq \frac{e}{\lfloor \frac{d_{in}-1}{2} \rfloor}$

Decode correctly if $\frac{e}{\lfloor \frac{d_{in}-1}{2} \rfloor} \leq \lfloor \frac{d_{out}-1}{2} \rfloor$

$\Rightarrow e \leq \lfloor \frac{d_{out}-1}{2} \rfloor \lfloor \frac{d_{in}-1}{2} \rfloor$

Developing intuition for the good decoding strategies:

Error patterns: ① Add d_{in} errors to as many blocks as possible

$\frac{e}{d_{in}}$ blocks which are erroneous.

outer code blocks which are corrupted $< \frac{d_{out}}{2}$

This can be corrected using the outer code.

② Add 0 errors or $\frac{d_{in}}{2}$ errors to each block.

$d(\hat{c}_i, y_i) \geq \frac{d_{in}}{2}$

Ignore this block and consider as erasures.

$\Leftarrow$

$\left\{ \frac{e}{d_{in}/2} \right\}$ Erasures $< d_{out}$

Claim: We can efficiently decode $RS(\mathbb{F}_q, n, K)$ code from τ errors & s erasures if $2\tau + s < n - K + 1$

s erasures — $RS(n-s, K)$

Use Berlekamp welch to decode τ errors.

FORNY'S GMD

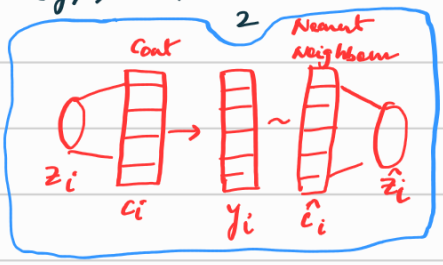
Codeword $c = (c_1 | c_2 | \cdots | c_N) \in C_{out}$

$c_i \in \Sigma_{in}^n$ $\quad n := n_{in}$ $\quad N := n_{out}$

Recieved $y = (y_1 | y_2 | \cdots | y_N)$

$c_i \longrightarrow y_i$

$d(y, C) < \frac{d_{in} \cdot d_{out}}{2}$



Nearest neighbour decoder for C_{in}

Erasure - Error decoder for C_{out} (R-S)

For $j = 1, 2, \ldots, N$; let $z_j = C_{in}^{-1}(c_j)$.

So, $(z_1 | z_2 | \cdots | z_N) \in C_{out}$

Let $\hat{c}_j$ be nearest codeword in C_{in} to y_j.

Let $\hat{z}_j = \mathcal{E}_{in}^{-1}(\hat{c}_j)$

$\theta = \{1, 2, \cdots, \lceil \frac{d_{in}}{2} \rceil\}$: Consider $\ell \in \theta$

$$X(\ell) = (x_1, \cdots, x_N) \in (\Sigma_{out} \cup \{?\})$$

for each j, $x_j = \begin{cases} \hat{z}_j & \text{if } d(y_j, \hat{c}_j) < \ell \\ ? & \text{o.w.} \end{cases}$

(ℓ sets the amount of allowed errors.)

Let s_ℓ = # of erasures in $X(\ell)$

r_ℓ = # of errors in the non erased coordinates

we need to show that $\exists \ell$ s.t. $2r_\ell + s_\ell < d_{out}$

we consider a probability distribution for ℓ, $\mathbb{P}$ over Θ

$\mathbb{E}_{\mathbb{P}}[2r_\ell + s_\ell] < d_{out}$

perceived errors → $w_j := d(y_j, \hat{c}_j)$

$\ell \in \Theta$, $\Psi_j(\ell) = \begin{cases} 0 & \text{if } c_j = \hat{c}_j \ \& \ w_j < \ell \quad \leftarrow \text{all fine} \\ 1 & \text{if } c_j \neq \hat{c}_j \ \& \ w_j < \ell \quad \leftarrow \text{incorrect decoding} \\ 1/2 & \text{if } w_j \geq \ell \quad \leftarrow \text{erasures} \end{cases}$ (Decoding Penalty)

$$r_\ell + \frac{s_\ell}{2} = \sum_{j=1}^{N} \Psi_j(\ell)$$

Probability Distribution → $\mathbb{P}(\ell = x) = \begin{cases} 2/d_{in} & \text{if } \ell \in \{1, 2, \cdots, \lfloor \frac{d_{in}}{2} \rfloor\} \\ 1/d_{in} & \text{if } \ell = \lceil \frac{d_{in}}{2} \rceil \end{cases}$ when d_{in} is odd

$$\mathbb{E}_{\mathbb{P}}\left[r_\ell + \frac{s_\ell}{2}\right] = \mathbb{E}_{\mathbb{P}}\left[\sum_{j=1}^{N} \Psi_j(\ell)\right] = \sum_{j=1}^{N} \mathbb{E}_{\mathbb{P}}[\Psi_j(\ell)] \leq \sum_{j=1}^{N} \frac{d(y_j, c_j)}{d_{in}} = \frac{d(y, c)}{d_{in}} < \frac{d_{out}}{2}$$

(will be shown)

① Case (I): $\hat{c}_j = c_j$ or $w_j \geq \lceil \frac{d_{in}}{2} \rceil$

$\hat{c}_j = c_j$: correct decoding

$w_j \geq \lceil \frac{d_{in}}{2} \rceil$: Guaranteed Erasure label

$\Psi_j = \begin{cases} 0 & \text{if } w_j < \ell \\ 1/2 & \text{if } w_j \geq \ell \end{cases}$

$$\mathbb{E}(\Psi_j) = \frac{1}{2}\mathbb{P}(\ell \leq w_j) = \frac{1}{2} \leq \frac{w_j}{d_{in}}$$

nearest decoding

$$\mathbb{E}(\Psi_j) \leq \frac{d(y_j, \hat{c}_j)}{d_{in}} \leq \frac{d(y_j, c_j)}{d_{in}}$$

② Case (II): $\hat{c}_j \neq c_j$ and $w_j < \lceil \frac{d_{in}}{2} \rceil$

Incorrect decoding, with two cases

$\Psi_j(\ell) = \begin{cases} 1 & \text{if } w_j < \ell \quad \leftarrow \text{Taking the incorrect} \\ 1/2 & \text{if } w_j > \ell \quad \leftarrow \text{Marking as erasure} \end{cases}$

$$\mathbb{E}(\Psi_j) = \mathbb{P}(w_j < \ell) + \frac{1}{2}\mathbb{P}(w_j \geq \ell)$$

$$= 1 - \frac{1}{2}\mathbb{P}(w_j \geq \ell) = 1 - \frac{1}{2}\frac{2}{d_{in}} w_j$$

$$= 1 - \frac{w_j}{d_{in}}$$

$$\mathbb{E}(\Psi_j) = \frac{d_{in} - d(y_j, \hat{c}_j)}{d_{in}} \leq \frac{d(y_j, c_j)}{d_{in}}$$

$\{ d(c_j, \hat{c}_j) \geq d_{in} \}$

triangle ineq.

$$d_{in} \overset{\text{code}}{\leq} d(c_j, \hat{c}_j) \leq d(y_j, c_j) + d(y_j, \hat{c}_j)$$

$I/p = (y_1 | y_2 | \cdots | y_N)$ $\quad o/p \to C \subseteq C_{out}$ or declare error

complexity

$N \cdot 2^{k_{in}} \cdot n_{in} \leq n^2$

N: Number of blocks; $2^{k_{in}}$: Each word of inner; n_{in}: getting distance

① ⓐ Apply Nearest Neighbour decoding to each inner code o/p block

$y_j \to \hat{c}_j$

ⓑ $\hat{z}_j = \mathcal{E}_{in}^{-1}(\hat{c}_j)$

② For $\ell = 1, 2, \cdots, \lceil \frac{d_{in}}{2} \rceil$

ⓐ $X(1), X(2), \cdots, X(n)$ s.t. $X(j) = \begin{cases} \hat{z}_i & \text{if } d(y_j, \hat{c}) < \ell \\ ? & \text{o.w.} \end{cases}$

Each has atmost polynomial

ⓑ Apply error-erasure decoder for C_{out} to decode from δ_ℓ erasures & $\tau_\ell = \left\lfloor \frac{1}{2}(d_{out} - 1 - \delta_\ell) \right\rfloor$ errors.

Get either $(z_1 | z_2 | \cdots | z_n) \in C_{out}$ or declare "error"

ⓒ Take the overall codeword

$$\hat{c} = (\mathcal{E}_{in}(z_1) | \mathcal{E}_{in}(z_2) | \cdots | \mathcal{E}_{in}(z_N))$$

Accept if $d(y, \hat{c}) \leq \frac{d_{in} d_{out}}{2}$ or declare "error"

Overall it is polynomial time.

BSC (p)

$\exists$ A random G matrix satisfies this.

$R^* < 1 - H(p)$

Explicit construction

Thm: BSC(p), small $\varepsilon > 0$

$\exists$ binary linear code (Concatinated code)

Inner code → GV bound
Outer code → Zyabulov bound s.t. $R \geq 1 - H(p) - \varepsilon$

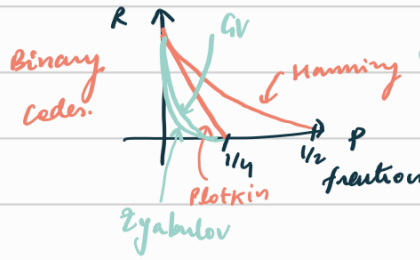
① Constructed explicitly in poly-time

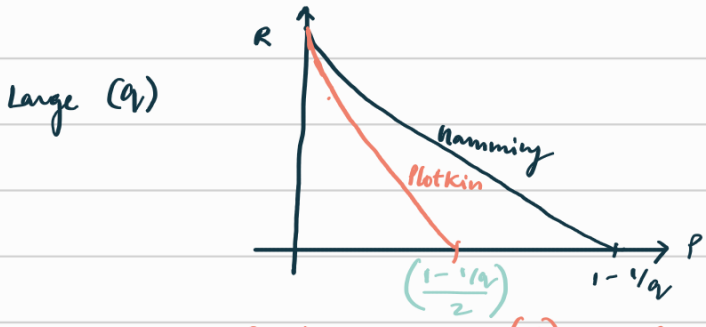
It itself is a concatenated code.

② Decoding in poly time & error probability decays exp. with n.

we donot use R.S. code because complexity becomes $n^{(\log n)}$, not a truly polynomial

List Decoding





$H_q(p) = p \log_q(q-1) - p \log_q(p) - (1-p) \log_q(1-p)$

Allow for a list of possible codewords/messages as o/p.
This list can be seen as a polynomial in n, not exponential.

Decoding: Let $p \in (0,1)$ (fraction of errors) and $L \geq 1$ (list size), A code $C \subseteq \Sigma^n$ is said to be (p, L) list decodable if $\forall y \in \Sigma^n$

$$\left\| \{ c \in C \mid d(y,c) \leq pn \} \right\| \leq L$$

find tradeoff of (R, p, L)

List decoding Capacity Theorem

Let $q \geq 2$, $p \in (0, 1-1/q)$, $\varepsilon > 0$

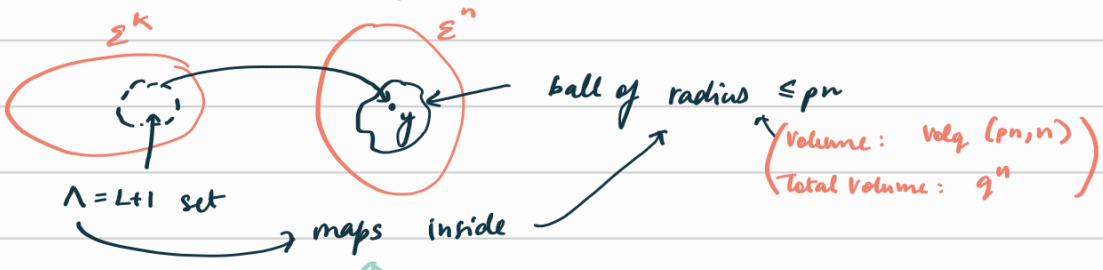
① If $R \leq 1 - H_q(p) - \varepsilon$, then $\exists$ a family of q ary

codes which are $(p, O(1/\varepsilon))$ - list decodable.
with rate R

② If $R \geq 1 - H_q(p) + \varepsilon$, every (p, L)-list decodable code of rate R has $L \geq q^{\Omega(n)}$

① Let C_R be a random map from $\Sigma^K \to \Sigma^n$

for a fixed p, find L s.t. it is list decodable.



we bound the probability of this bad event:

$$\mathbb{P}(\text{Bad event}_{\Lambda, y}) = \mathbb{P}\left(\bigcap_{i=1}^{L+1} \{M_i \to B(y, pn)\}\right)$$

$$\{\text{each is mapped uniformly at random}\} = \left(\frac{\text{Vol}_q(pn, n)}{q^n}\right)^{L+1}$$

$$\left\{\binom{q^K}{L+1} \cdot (q^n)\right\}$$

↑ choices of Λ ↑ choices of y

$$\mathbb{P}(\text{Bad event}) \leq \binom{q^K}{L+1} \cdot q^n \cdot \left(\frac{\text{Vol}_q(pn, n)}{q^n}\right)^{L+1}$$

$$\leq (q^K)^{L+1} \cdot q^n \cdot q^{\{n H_q(p) - n)(L+1)}$$

$$= q^{\{KL + K + 1 + n H_q(p)(L+1) - nL - 1\}}$$

$$= q^{n\{(R - 1 + H_q p)(L+1) + 1\}}$$

$$\leq q^{n\{-\varepsilon(L+1) + 1\}} \leq q^{-n\varepsilon} \to 0$$

{exponentially fast goes to 0}

As long as $L \geq \Omega(1/\varepsilon)$

$\hookrightarrow L \geq c/\varepsilon$

where c is some constant

② Suppose $C \subset \Sigma^n$ with rate $R \geq 1 - H_q(p) + \varepsilon$

$\exists\, y \in \Sigma^n$ s.t. $|C \cap B(y, pn)| > L$ (is large $L \geq q^{\Omega(n)}$)

choose y - uniformly at random

↳ E of the quantity is larger.

Fix $c \in \mathcal{C}$

$$\mathbb{P}\left(c \in B(y, \rho n)\right) = \mathbb{P}\left(y \in B(c, \rho n)\right) = \frac{\mathrm{Vol}(\rho n, n)}{q^n} \approx q^{-n(1-H_q(\rho))}$$

$$\mathbb{E}\left(|\mathcal{C} \cap B(y, \rho n)|\right) = q^k \cdot q^{-n(1-H_q(\rho))} \geq q^{n(1-H_q(\rho)+\varepsilon)} \cdot q^{-n(1-H_q(\rho))} = q^{n\varepsilon}$$

$$\Rightarrow \quad L \geq q^{n\varepsilon - o(n)}$$

Johnson Bound

Any code with good relative distance, it is also a "good" code for list-decodability.

Thm: $J_q(\delta) = \left(1 - \frac{1}{q}\right)\left(1 - \sqrt{1 - \frac{q\delta}{q-1}}\right)$

Let $C \subset \Sigma^n$ be some code with relative distance δ

Then if $\rho < J_q(\delta)$, then C is $(\rho, q\delta n^2)$ - list decodable.

Pf: $q = 2$ Any binary code C with minimum distance d,

$y \in \{0,1\}^n$, $|C \cap B(y, \rho n)| \leq 2dn$

for $\rho < \frac{1}{2}(1 - \sqrt{1-2\delta})$

Take C (codeword), y (or received word).

Say, $c_1, c_2, \ldots, c_M \in B(y, \rho n)$

Let $c_i' = c_i - y$

① $\mathrm{wt}(c_i') \leq \rho n$

② $d(c_i', c_j') \geq d \quad \forall i \neq j$

$$S = \sum_{i<j} d(c_i', c_j') \quad \Rightarrow \quad S \geq \binom{M}{2} d$$

$$S = \sum_{i=1}^{n} m_i (M - m_i) \qquad \sum_{i=1}^{n} m_i \leq n\rho M$$

where $m_i = \#$ 1s in the i^{th} row

$\Rightarrow \quad S \leq M^2 np(1-p)$

$\Rightarrow \binom{n}{2} d \leq M^2 np(1-p)$

$\Rightarrow \quad M \leq \dfrac{2dn}{(n-pn)^2 - n(n-2d)}$

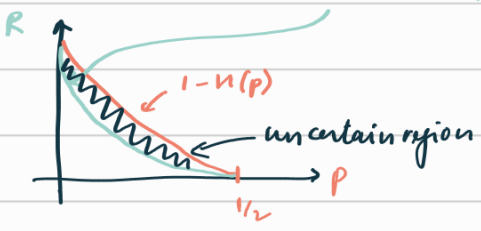
$p < \frac{1}{2}\left(1 - \sqrt{1 - \frac{2d}{n}}\right)$ $\qquad \leq 2dn$ for $p < J_2(\delta)$

$2pn < n - \sqrt{n(n-2d)}$

GV bound: $\exists$ code s.t. $\delta = H^{-1}(1-R)$

$\hookrightarrow \quad p \leq \frac{1}{2}\left(1 - \sqrt{1 - 2H^{-1}(1-R)}\right)$

$\Rightarrow R < 1 - H(2p(1-p))$



for large q, $H_q(p) \approx p$

LDC capacity $\rightsquigarrow 1 - H_q(\delta) = 1-p$

JB $\longrightarrow \quad J_q(\delta) = 1 - \sqrt{1-\delta}$

$p < 1 - \sqrt{1-\delta}$

or $p < 1 - \sqrt{R}$ {if MDS code}

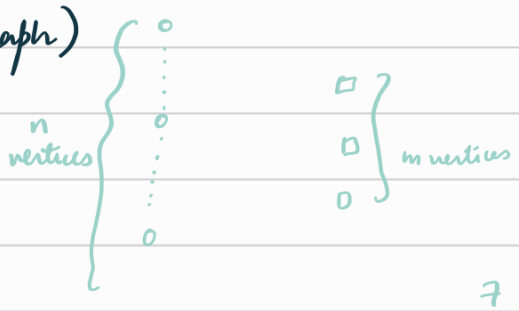
or $R < (1-p)^2$

Graph - Based code

Factor graph: Take any (n, k) code $= n - m$

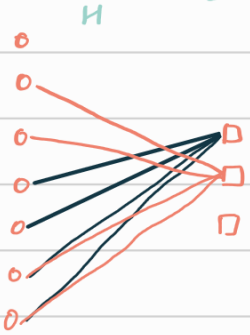
↑ (Bipartite graph)

H - parity check matrix $\in \{m \times n\}$



(7, 4) Hamming Code: H (7 columns, 3 rows)

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



Low density parity check codes ← when the factor graphs are sparse. (no. of edges linear in n)

→ d- regular graph if all vertices have a degree d.

d- left regular ← all in left have degree d

D- right regular ← all in right have degree D

→ $S \subseteq V$

$w \in V \setminus S$ w is a neighbour of atleast one vertex in S then w is a neighbour of S.

$N(S)$ ← Set of neighbours of S

$S \subset L \Rightarrow N(S) \subset R$

Unique Neighbour: $S \subseteq V$

$w \in V \setminus S$

w is a unique neighbour of S if it is adjacent to EXACTLY one vertex in S.

Bipartite Expander Graph

Every "small" set of vertices in L have a "large" set of neighbours in R.

Def^n: An $(n, m, D, \gamma, \alpha)$ - bipartite graph is a D-left regular bipartite graph $G(L \cup R, E)$, $|L| = n$, $|R| = m$ $\{m \leq n.\}$

$\rightarrow \forall\ S \subseteq L$, $|S| \leq \gamma n$ have $|N(S)| \geq \alpha |S|$

"Expander"

Left sets of smaller than γ fractional size, have a neighbourhood of atleast α times larger.

Implications:

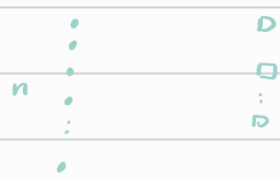
$\alpha \leq D$ if $\alpha = D \Rightarrow \gamma n D \leq m \Rightarrow \gamma \leq \frac{m}{nD}$

Probabilistic Argument

Thm: $\varepsilon > 0$, $m \leq n$, $\exists\ \gamma > 0$ and $D \geq 1$ s.t. an $(n, m, D, \gamma, D(1-\varepsilon))$ bipartite expander graph exists with $\gamma = \frac{m}{nD e^{1/\varepsilon}}$, $D = f(\varepsilon) \cdot \log(n/m)$ ↑ some function of ε.

$R = 1 - \frac{m}{n}$

Proof:



Graph is created by randomly choosing D neighbours each vertex in L

For $S \subseteq L$ & $M \subseteq R$, $P_{S,M} = \mathbb{P}(N(S) \subseteq M)$

$\leq \left(\frac{|M|}{m}\right)^{D \cdot |S|}$

Bad Event $\exists\ S \subseteq L$, $|S| \leq \gamma n$ for which $\exists\ M$ s.t. $|M| < \alpha |S|$ & $|N(S)| \leq M$

$$\mathbb{P}(\text{Bad event}) \leq \sum_{\substack{S \subseteq L \\ |S| \leq \gamma n}} \sum_{\substack{M \subseteq R \\ |M| = \alpha |S|}} P_{S,M}$$

$$\leq \sum_{s=1}^{\gamma n} \binom{n}{s} \binom{m}{\alpha s} \left(\frac{\alpha s}{m}\right)^{Ds}$$

$$\leq \left(\frac{nD\, e^{1+1/\varepsilon}}{m}\right) (1-\varepsilon)^{\varepsilon D}$$

Claim: Let G be an $(n, m, D, r, D(1-\varepsilon))$ bipartite expander graph for $\varepsilon < 1/2$, then the code C corresponding to G satisfies $d(C(G)) \geq 2r(1-\varepsilon)n$

↳ Asymptotically good code.

Claim: Let G be an $(n, m, D, r, D(1-\varepsilon))$ bipartite expander graph with $\varepsilon < 1/2$. For any $S \subseteq L$ with $|S| \leq rn$, $|U(S)| \geq D(1-2\varepsilon)|S|$

($U(S)$: unique neighbours)

$\rightsquigarrow |N(S)| \geq D(1-\varepsilon)|S|$

Sketch: There are D for left node and atmax εD of them can be repeated to maintain expander property. Therefore, $(1-2\varepsilon)D$ will be unique.

Proof: # edges out of $S \rightarrow D|S|$

out of $D|S|$, atleast $D(1-\varepsilon)|S|$ go to unique vertices in $R(S)$

$\rightarrow \varepsilon D|S|$ edges are remaining

$|N(S)|$

unique neighbours : $|U(S)| \geq D(1-\varepsilon)|S| - \varepsilon D|S|$

Minimum distance grows atleast $> r \cdot n$

$|S| \leq rn$ ↑ set where it is one.

if $U(S) \neq \emptyset$, then cannot be a codeword.

Any word $\equiv$ set of left nodes

For codewords $\Rightarrow$ # Uniques $= 0$. (One way)

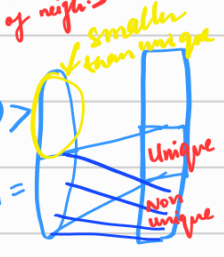
Claim: Let G be an $(n, m, D, r, D(1-\varepsilon))$ expander with $\varepsilon < 1/2$. Then $d(C(G)) \geq 2r(1-\varepsilon)n$.

{If $\neq 0$, then there will be that parity check not satisfied}

Pf: Assume $d(C) < 2r(1-\varepsilon)n$ (C a codeword) ↑ The smallest set which has no unique neighbours & each has an even # of neigh.

S to be the set corresponding to 1^s in C.

$U(S)$ corresponds to unsatisfied parity checks.



① $|S| \leq rn \rightarrow |U(S)| \geq 1$ $\Rightarrow$ contradiction

② $\left\{ \begin{array}{l} |S| > rn \\ |S| < 2r(1-\varepsilon)n \end{array} \right\} \rightarrow$ Choose $Q \subseteq S$, $|Q| = rn$

$|U(Q)| \geq D(1-2\varepsilon)rn$

$|S \setminus Q| < 2r(1-\varepsilon)n - rn = r(1-2\varepsilon)n$

no. of neighbours of $S \setminus Q$ is $< Dr(1-2\varepsilon)n$

Assume they all are in $U(Q)$, still we will have one in $U(Q)$ which has 1 neighbour.

$\Rightarrow$ $|S| < 2r(1-\varepsilon)n$ has $U(S) \neq \phi$. ∎

$R = 1 - \frac{m}{n} = 1-\beta$; $m = \beta n$, $0 < \beta < 1$

$\delta > c$ $\Rightarrow$ Asymptotically good code.

Decoding

Claim: Decoding algorithm can efficiently correct $< r(1-2\varepsilon)n$ errors, $\varepsilon < 1/4$.

$nr(1-2\varepsilon)$

Algo: while $\exists\ y \in L_G$ which has # unsatisfied checks > # satisfied checks

Flip v_y & update the list of checks.

Claim: If assignment on L_G has $< rn$ errors (and ≥ 1), then $\exists$ a vector $y \in L_G$ s.t. # unsatisfied checks > # satisfied checks.

{use of expanding property}

Pf: $T \subseteq L_G$ → set of error locations $|T| < rn$

$\Rightarrow$ $|U(T)| \geq D(1-2\varepsilon)|T| > D/2|T|$ (as $\varepsilon < 1/4$)

↑ These checks are unsatisfied. There could be more.

$\Rightarrow$ $\exists\ t \in T$ s.t. unsatisfied checks of $t > \frac{D}{2}$

(As avg. is larger, atleast one of the should be as well.) $\Rightarrow$ satisfied checks $< \frac{D}{2}$ ∎

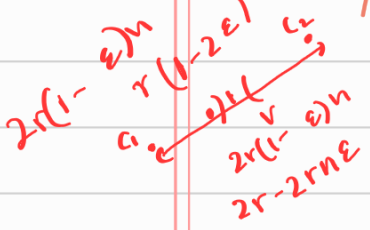
Claim: We never reach an assignment to L_G with $\geq rn$ errors.

Pf: Recieved word $x < r(1-2\varepsilon)n$ errors.

unsatisfied checks in beginning $< Dr(1-2\varepsilon)n$

Suppose reach a word with rn errors

$\Rightarrow$ # unsatisfied checks $\geq D(1-2\varepsilon)rn$.



Not possible as the number of unsatisfied checks is always decreasing.

Claim: we cannot get to another codeword, i.e. decoding is correct. ($> 2r(1-\varepsilon)n$)

Proof: As we have a bound on the distance and it cannot go above rn, we cannot get a wrong codeword out of it.

Received is close to codeword, when we change the no. of unsatisfied checks strictly decrease. To get to the other c.w., it has to increase.

Complexity: (A) Pre processing

D left regular, d-max degree in R_G

① Parity checks in $R_G \to O(d \cdot m)$

② $Q \to$ vertices with more unsatisfied than satisfied.

↳ $O(D \cdot n) = O(D \cdot md)$

(B) Each iteration: → update checks: $O(D)$

at most m iterations

update list: $O(D \cdot d)$

⟶ $O(m \cdot d \cdot D)$

⇒ Total: $O(\underbrace{m \cdot d \cdot D}_{\text{constants}}) \sim O(n)$

Tanner Codes: They generalize

G – D left, d-right

$C_0 \subseteq \mathbb{F}_2^d$

Code → $X(G, C_0) = \{c \in \mathbb{F}_2^n : \forall u \in R_G \; c|_{N(u)} \in C_0\}$

G – D left regular

d right regular

Restriction to

$C_0 \to (d, d-1, 2)$

↑ The one we studied as expander codes.

G will require expansion factor of $D/d(G)$

Reduces the expansion factor.

Group testing

n items, $\leq k$ defectives

$m \left[\quad \right]_{n} \left[\begin{matrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{matrix} \right] \leftarrow$ defectives by "1" $= \left[\quad \right]$ m test outputs

Pooling matrix Φ

Addition is OR, multiplication is AND

at least one $\Leftrightarrow$ 1 defective

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

Adaptive test

Tests are run sequentially.

① $t = 1 \rightarrow$ Binary search $\leq \log_2 n$ tests

items into 2 halves: $n/2$ | $n/2$ → $n/4$ $n/4$

② $t \geq 1 \rightarrow \leq t \log_2 n$ tests

Lower Bound ← m tests, t defectives out of n

Defective patterns $\binom{n}{t}$ ⇄ Outputs $\leq 2^m$

Valid function from outputs to inputs.

$\Rightarrow 2^m \geq \binom{n}{t} \geq \left(\frac{n}{t}\right)^t$

$\Rightarrow m \geq t \log \frac{n}{t}$

"Best" can be achieved.

$O\left(t \log \frac{n}{t}\right)$ tests is state-of-the-art.

Non adaptive

$m \left[\quad \overset{n}{\Phi} \quad \right] \left[x \right] = \left[y \right]$

$t = 1$

$\log (n+1) = m$ $\begin{bmatrix} 0 & 0 & \cdots & \cdots \\ 0 & \vdots & & \\ 1 & 0 & & \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \end{bmatrix}$

can use parity check matrix of Hamming code.

② $t > 1$

t-Disjunct matrix: $m \times n$ binary matrix, said to be t-Disjunct if union of any t columns doesn't contain any other single column.

$$\begin{matrix} & n \\ m & \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{matrix} \leftarrow 2 \text{ disjunct matrix}$$

Union of these two, doesn't cover any other two.

Property: t-disjunct matrix for any set $\Lambda \subseteq [n]$ of size t and any $j \in [n] \setminus \Lambda$, then $\exists\, i \in [m]$ s.t. $\Phi_{ij} = 1$ & $\Phi_{i\ell} = 0 \quad \forall\, \ell \in \Lambda$

↳ $\exists$ a test "i" of non defectiveness of j.

Claim: If Φ is an $(m \times n)$ t-disjunct matrix, then it can be used to identify upto t defective using an algo in complexity $O(mn)$.

Pf: For $j \in [n]$,

if all tests including j are positive, then mark defective

else: mark non defective.

Construct $m \times n$ disjunct matrices.

Best lower bound on $m \to \Omega\left(\frac{t^2 \log n}{\log t}\right)$ { D

{ Seperability and stuff is needed to argue a need of a disjunct matrix for any test number achieves. }

Randomized Construction of t-Disjunct matrix

$m \times n \longrightarrow$ entry $\sim$ Ber (p) i.i.d.

↳ Find probability of property

Fix Λ of t columns, $j \in [n]$

Prob that condition not satisfied for Λ, j $= \left(1 - \underbrace{(1-p)^t p}_{\text{not happening for 1 row}}\right)^{m}$ ← for all row

Prob (Matrix is not t-disjunct) $\leq \binom{n}{t+1}(t+1)\left(1-(1-p)^t p\right)^m$

$p^* = \frac{1}{t+1}$ $= \binom{n}{t+1}(t+1)\left(1-\frac{t^t}{(t+1)^{t+1}}\right)^m$

If $m = \Omega\left(t^2 \log \frac{n}{t}\right) \Rightarrow Pr \to 0$ as $n \to \infty$

Explicit Constructions

$m = O(t^2 \log_t^2 n)$

$m = O(t^2 \log e^n)$

$m = O\left(t^2 \frac{\log^2 n}{\log t}\right)$

(Random disjective model)

← Random Errors V/s Adversarial Errors

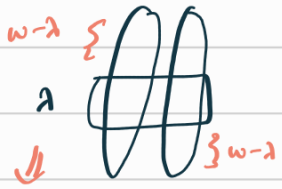
That's why better

Claim: Consider a constant weight code C with weight w & min dist: d

λ = max overlap b/w any pair of codewords

$\lambda \leq w - d/2$

$\{ 2(w-\lambda) \geq d \}$



Proof: $\Downarrow$

$2(w-\lambda) \geq d$

Claim: Φ is t-disjunct if $t\lambda < w$

or $t < w/\lambda$.

Proof: Set S

t

$t\lambda < w \Rightarrow t$ disjunct.

If we have $t < \frac{w}{w - d/2} \Rightarrow t < \frac{w}{\lambda} \Rightarrow t$ disjunct.

Concatenated Code

Code = q- any RS code of dim K & length q

Inner code: 2^q ← not linear

(2) $0 \to 0 \cdots 01$

$1 \to 100 \cdots 0$

$2 \to 010 \cdots 0$

$q-1 \to 00 \cdots 10$

$n = q^2$, $w = q$, $d = 2(q-K+1)$

$$t = \frac{w}{w - d/2} = \frac{q}{q - (q-k+1)} = \frac{q}{k-1}$$

$$= \frac{\sqrt{n}}{\log n \log \sqrt{m}}$$

$$t \approx \frac{\sqrt{m} \log \sqrt{m}}{\log n}$$

$$\Downarrow$$

$$m \approx \Omega\left(t^2 \log_t n\right)$$