Non-linear Codes

- Codes used to correct ~~xx~~ errors on noisy communicat- Channels.
- linear codes $\longrightarrow$ several practical advantages
  $[n, k, d]$ or (n, q^k, d)
- Nonlinear codes $\longrightarrow$ largest possible # of codewords
  (n, M, d) with a given min-dist.
  $[A_q(n, d)]$.

Def^n. ~~Non-linear Code~~

(n, M, d) code is a set of M codewords of length n (with components from some field F) s.t. any two vectors differ in at least d places, and d is the largest no. with this property.

- No co-ordinate place in which every codeword is 0 (otherwise it would be an $(n-1, M, d)$ code).
- $c_1 \sim c_2 = (c_1 + d) \sim (c_2 + d)$
  $\text{dist.}(c_1 \sim c_2) = \text{dist}\big((c_1+d) \sim (c_2+d)\big)$, for some const. d & $c_1, c_2 \in \mathcal{C}$.
- Code contains the zero vector.
- Equivalent codes

two (n, M, d) codes $\mathcal{C}, \mathcal{D}$ are equivalent if one can be obtained from the other by permuting the n symbols & adding a const. vector.

- π be a permutation, a be a vector
  $$\mathcal{D} = \{ \pi(u) + a : u \in \mathcal{C} \}$$

Claim

Example:

000		111
011	and	100
101		010
110		001

equivalent codes $(a = 111)$

More generally (equivalence of non-binary codes)

- $\mathcal{C}, \mathcal{D} \rightarrow$ codes of length n over a field F of q elements.
- $\mathcal{C}$ & $\mathcal{D}$ are equivalent if $\exists$ n permutations $\pi_1, \dots, \pi_n$ of the q elements & a permutation σ of the n ~~coo~~ co-ordinates positions s.t. if $(u_1, u_2, \dots, u_n) \in \mathcal{C}$ then $\sigma(\pi_1(u_1), \dots \pi_n(u_n)) \in \mathcal{D}$.
- if $\mathcal{C}, \mathcal{D}$ both are linear, then only those π_i generated by scalar multiples & field automorphisms can be used

Weight Distribution

- $A_i \rightarrow$ # of codewords of wt. i of an (n, M, d) code
- $A_0, A_1, \dots, A_n \rightarrow$ weight distribution of $\mathcal{C}$.

$$A_0 + A_1 + \dots + A_n = M.$$

(MacWilliams identities will be studied later)

$\{00, 01, 11\} \longrightarrow$ Not distance invariant.

$A_0 = 1$, $A_1 = 1$, $A_2 = 1$.

00 → 01: $A_1 = 1$ codeword at $\boxed{\text{dist. } 1}$

00 → 11: $A_2 = 1$ codeword at $\boxed{\text{dist. } 2}$

01 — 00, 11: 2 codewords at $\boxed{\text{distance } 1} \neq A_1$

~~0 vector~~ ~~other vector~~

~~A_i codewords at dist i~~

- observer sitting on 0 would see A_i codewords at distance i from him.
- for linear code, the view is same from any codeword. (why?) $x_1, x_2 \in \mathcal{C} \Rightarrow x_1 - x_2 \in \mathcal{C}$
  $\longrightarrow$ distance invariant
- for non-linear code, this need not be true.

Distance Distribution

- $B_0, B_1, \ldots, B_n$ when
$$B_i = \frac{1}{M}\left[\#\text{ of ordered pairs of codewords } u, v \text{ s.t. } \operatorname{dist}(u,v) = i\right]$$
- $B_0 = 1 \longrightarrow \frac{1}{M}\left[\#\ (u,u) \in \mathcal{C}^2\right] = \frac{M}{M} = 1$

$B_0 + B_1 + \cdots + B_n = M$.

- for linear codes, the weight & distance distributions coincide.
- A translated code $a + \mathcal{C}$ has the same dist. distribution as $\mathcal{C}$.

Claim $A(n,d) = 2\left\lfloor \frac{d}{2d-n} \right\rfloor$ if $2d > n \geq d$.

The Plotkin bound

Theorem for any (n, M, d) code $\mathcal{C}$ for which $n < 2d$, we have

$$\boxed{M \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor}.$$

proof. Calculate the sum $S = \sum_{u \in \mathcal{C}} \sum_{v \in \mathcal{C}} \text{dist}(u, v)$ in two ways.

$\text{dist}(u,v)$ & $\text{dist}(v,u)$

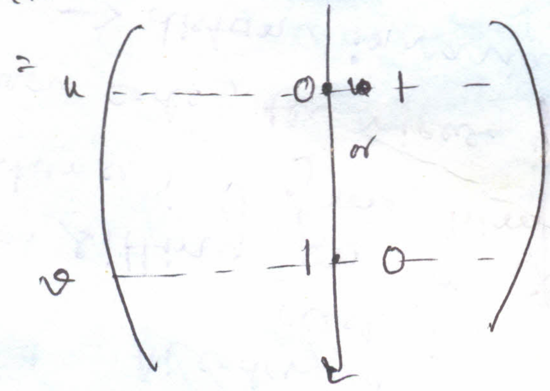
$\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$ $1+2+1=4$

$2.2.1 + 2.1.2 = 4+4 = 8$

- $\text{dist}(u,v) \geq d$ if $u \neq v$.

$\therefore S \geq M(M-1)d$.

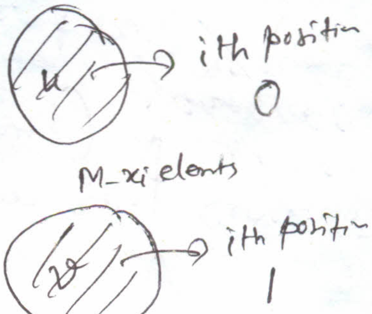
- $A_{M \times n} \to$ rows are codewords.



$2+2+2+2+2+2 = 12$

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

$\sum 2.2.(4-2) + 2.2.(4-2) + 2.2(4-2) = 3 \times 8 = 24$.



x_i elements, ith position 0

$M - x_i$ elements, ith position 1

i-th column $\to x_i$ 1's, $M - x_i$ 0's $\hookrightarrow$ contribute

Contains x_i 0's & $M - x_i$ 1's.

$\hookrightarrow$ contributes $2(M-x_i)x_i$ to the sum S.

$$\therefore S = \sum_{i=1}^{n} 2x_i(M - x_i)$$

$\left(\frac{\partial S}{\partial x_i} = 0 \;\forall\, i = 1, 2, \ldots, n\right)$ $2 \cdot \frac{M}{2} \cdot \frac{M}{2}$

Case I (M even) S is maximum ~~when~~ if all $x_i = \frac{M}{2}$

& $S_{max} \leq \frac{1}{2} n M^2$ $\quad S_{max} = \frac{1}{2} n M^2$

Thus we have

$$M(M-1)d \le \frac{1}{2} n M^2$$

$M - x_i - x_i = 0$
$x_i = \frac{M}{2}$.

or $d(M-1) \le \frac{1}{2} n M$ $\Rightarrow 1 - \frac{1}{M} \le \frac{n}{2d}$

$\Rightarrow -\frac{1}{M} \le \frac{n}{2d} - 1$

$\Rightarrow -M \ge \frac{-2d}{2d-n}$.

$\Rightarrow \boxed{M \le \frac{2d}{2d-n}}$

$M \le 2 \times 2.4 = 4.8$
M even
$M \le 2[2.4] = 4$

M even
$\Rightarrow M \le 2\left[\frac{d}{2d-n}\right]$

Case II (M odd).

$$S \le n \frac{(M^2-1)}{2}$$

$\frac{\partial S}{\partial x_i} = 0, \; i = 1, 2, \ldots, n$

$\Rightarrow M - x_i - x_i = 0$

$\Rightarrow x_i = \left[\frac{M-1}{2}\right]$

$\therefore S_{max} = \frac{1}{2}\left(\frac{M-1}{2}\right)\left(\frac{M+1}{2}\right)$

$= \frac{1}{2}\left(\frac{M^2-1}{2}\right)$

Thus we have,

$$M(M-1)d \le \frac{n}{2}(M^2-1).$$

$\frac{2d}{n} \le \frac{M^2-1}{M^2-M}$

$\frac{2d}{n} - 1 \le \frac{M^2 - 1 - M^2 + M}{M^2 - M} = \frac{1}{M+1}$

$\therefore M+1 \le \frac{n}{2d-n}$.

or $M \le \frac{n}{2d-n} - 1 =$

$$Md \le \frac{n}{2}(M+1) \Rightarrow M\frac{2d}{n} - M \le 1$$

$$M \le \frac{1}{\frac{2d}{n} - 1} = \frac{n}{2d-n} = \frac{2d}{2d-n} - 1$$

$[2 \times 2.4] = [4.8] = 4$
$= 2[2.4] = 4$

$[2x] = 2[x]$

$[2 \times .4] = [.8] = 0$
$= 2 \times [.4] = 0$

$$\boxed{M \le 2\left[\frac{d}{2d-n}\right]}$$

$\le \left[\frac{2d}{2d-n}\right]$

using $[2x] \le 2[x] + 1$

$1.3 < [1.3]$

$[2 \times 1.3]$
$= [2.6]$
$\le 2 \cdot [1.3] + 1$
$2 + 1 = 3$.

$1.3 < [1.3] = 1$

Binary ($q=2$).

- $A(n,d) \rightarrow$ largest # M of codewords in any (n,M,d) code.

$\rightarrow$ enough to find $A(n,d)$ for even value of d.

Theorem

$$\boxed{A(n, 2r-1) = A(n+1, 2r).}$$

Proof: Let $\mathcal{C}$ be an $(n, M, 2r-1)$ code

$\downarrow$ add overall parity

$(n+1, M, 2r)$ code.

$\therefore A(n, 2r-1) \leq A(n+1, 2r)$. $\longleftarrow$ (1)

Sub class

$\mathcal{C}_i \rightarrow \mathcal{C}_i'$

$(n, 2r-1)$ $\quad$ $(n+1, 2r)$

$A(n, 2r-1)$ $\quad \leq \hookrightarrow A(n+1, 2r)$

Conversely, given $(n+1, M, 2r)$ code

$\downarrow$ delete one co-ordinate

$(n, M, d \geq 2r-1)$ $\longleftarrow$ (1)

$\therefore A(n+1, 2r) \leq A(n, 2r-1)$ $\longleftarrow$ (2)

(1), (2) $\rightarrow$ the result

$M = A(n,d)$

~~$M = A(n,d)$~~

Theorem

$$\boxed{A(n,d) \leq 2A(n-1,d)}$$

Proof: $\mathcal{C} \rightarrow (n, M, d)$ code

A: all codewords begin with 0 — class 1 $\quad < \frac{A(n,d)}{2}$

B: all codeword begin with 1 — class 2 $\quad \geq \frac{A(n,d)}{2}$

- if $|A| < \frac{A(n,d)}{2}$, then $|B| \geq \frac{A(n,d)}{2}$

~~$A(n-1,d) \leq \frac{1}{2}A(n,d)$~~ $\hookrightarrow$ delete 1st. co-ordinate

$$A(n-1, d) \geq \frac{A(n,d)}{2}$$

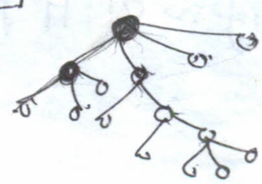
if $|B| < \frac{A(n,d)}{2}$ then $|A| \geq \frac{A(n,d)}{2}$

delete 1st co-ordinate 0

$$A(n-1, d) \geq \frac{1}{2} A(n,d)$$

u,v – 5 dist. apart
⇒ u,v – 3 dist. apart also.

[d → two vectors differ at least d places & d is largest no. with this property.]



<u>Corollary</u> (The Plotkin bound)

- If d is even and $2d > n$, then

(1) — $A(n,d) \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor$ (proved already)

(2) — $A(2d,d) \leq 4d$ ⟶ $d=2r$, $A(4r, 2r) \leq 2A(4r-1, 2r)$ by above Th. ($n < 2d$)

$\leq 4 \left\lfloor \frac{2r}{4r-(4r-1)} \right\rfloor = 8r = 4d.$

- If d is odd and $2d+1 > n$, then

(3) — $A(n,d) \leq 2 \left\lfloor \frac{d+1}{2d+1-n} \right\rfloor$ ⟶ d odd so $d+1$ even

$A(n,d) = A(n+1, d+1)$

$\leq 2 \left\lfloor \frac{d+1}{2(d+1)-(n+1)} \right\rfloor$

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

(4) — $A(2d+1, d) \leq 4d+4$ → can be shown similarly

⟶ $A(2d+1,d) = A(2d, d-1) \leq 2 \left\lfloor \frac{d-1}{2(d-1)-2d} \right\rfloor$

$= A(2d+2, d+1)$

$= A(2(d+1), d+1)$

$\leq 4(d+1) = 4d+4.$

- If Hadamard matrices exist of all possible order (open problem still), then equality holds in (1)–(4).
- Plotkin's Bound is tight (Levenshtein's theorem)

i.e. ∃ codes which meet this bound. provided enough Hadamard matrices exist.

Claim $A(n,d) = 2\left\lfloor \frac{d}{2d-n} \right\rfloor$ if $2d > n \geq d$.

Hadamard matrices & Hadamard codes

- $H_{n \times n}$ of $+1$'s & -1's s.t. $HH^T = nI$.
  - ↳ Hadamard matrix (H_n)
    - → distinct rows (/columns) are orthogonal
    - → real inner product of any row with itself is n.
    - → multiplying any row (/column) of H by -1 yields another Hadamard matrix
- Normalized Hadamard matrix → 1st. row, 1st. column all $+1$.

Examples

$$H_1 = (1), \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \quad H_4 = \left(\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ \hline 1 & 1 & - & - \\ 1 & - & - & 1 \end{array}\right)$$

$$H_8 = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ \hline 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{array}\right), \quad H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}.$$

Theorem If a Hadamard matrix H of order n exists, then n is 1, 2 or a multiple of 4.

proof.

H → normalized

$n \geq 3$, the composition of the 1st. three rows of H is as follows:

interchanging columns ←

$$\underbrace{\begin{matrix} 1\,1 \cdots 1 \\ 1\,1 \cdots 1 \\ 1\,1 \cdots 1 \end{matrix}}_{i} \quad \underbrace{\begin{matrix} 1\,1 \cdots 1 \\ 1\,1 \cdots 1 \\ - - \cdots - \end{matrix}}_{j} \quad \underbrace{\begin{matrix} 1\,1 \cdots 1 \\ - - \cdots - \\ 1\,1 \cdots 1 \end{matrix}}_{k} \quad \underbrace{\begin{matrix} 1\,1 \cdots 1 \\ - - \cdots - \\ - - \cdots - \end{matrix}}_{l}$$

Since the rows are orthogonal, we have

$$\left.\begin{array}{l} i+j-k-l=0 \\ i-j+k-l=0 \end{array}\right\} \overset{(+)}{\Rightarrow} \begin{array}{l} i=l \\ j=k \end{array} \qquad i=j=k=l$$

$$i-j-k+l=0$$

$i-j$, $k=l$

$\therefore n = 4i$ is a multiple of 4.

<u>Conjecture</u>: Hadamard matrices exist whenever the order is a multiple of 4. (not yet proved).

- Smallest order $n = 268$ for which a Hadamard matrix has not been constructed.

<u>Two constructions</u>

- <u>The Sylvester construction</u>.
  - If H_n is a Hadamard matrix of order n then $H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$ is a Hadamard matrix of order $2n$. $\longrightarrow$ Sylvester matrices.

- $H_1, H_2, H_4, H_8, H_{16}, H_{32}$, H_{12}, H_{20}, H_{24}, H_{28}

- <u>The Paley Construction</u>. (uses quadratic residues)
  - This construction gives a Hadamard matrix of any order $n = p+1$ which is a multiple of 4 (or of order $n = p^m+1$ if we use quadratic residues in $GF(p^m)$).
  - $H = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & Q-I \end{pmatrix}$, $Q_{p\times p} = (q_{ij})$, $q_{ij} = \chi(j-i)$

H: Hadamard matrix of order $n = p+1$

Q: Jacobsthal matrix of order $p = n-1$.

χ: Legendre Symbol

~~Example: p=7~~

Quadratic Residues

- $p \to$ odd prime
- $Z_p^* = \{1, 2, \dots, p-1\}$
- $1^2, 2^2, \dots$ mod $p \to$ quadratic residues mod p
- $\frac{p-1}{2}$ elements of $Z_p^* \in QR_p$ $\quad 1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$ mod p

$\frac{p-1}{2}$ elements of $Z_p^* \in QNR_p$.

Example: $p = 11$

$$\left.\begin{array}{l} 1^2 = 1 \\ 2^2 = 4 \\ 3^2 = 9 \\ 4^2 = 16 = 5 \\ 5^2 = 25 = 3 \end{array}\right\}$$

$QR_{11} = \{1, 4, 9, 5, 3\}$

$QNR_{11} = \{2, 6, 7, 8, 10\}$

$$\left.\begin{array}{l} (11-5)^2 \leftarrow 6^2 = 36 = 3 \\ (11-4)^2 \leftarrow 7^2 = 49 = 5 \\ (11-3)^2 \leftarrow 8^2 = 64 = 9 \\ 9^2 = (11-2)^2 = 4 \\ 10^2 = (11-1)^2 = 1 \end{array}\right\}$$

$\chi(66) = 0$ as $66 \bmod 11 = 0$

$\chi(50) = -1$ as $50 \bmod 11 = 6 \in QNR_{11}$

$\chi(25) = 1$ as $25 \bmod 11 = 3 \in QR_{11}$

Legendre symbol χ

$$\chi(i) = \begin{cases} 0 & \text{if } i \bmod p = 0 \\ 1 & \text{if } i \bmod p \in QR_p \\ -1 & \text{if } i \bmod p \in QNR_p \end{cases}$$

$\chi(xy) = \chi(x)\,\chi(y)$ for $0 \le x, y \le p-1$

~~orem~~

for any $c \not\equiv 0 \mod p$, $\sum_{b=0}^{p-1} \chi(b)\chi(b+c) = -1$

proof - • $b=0$ contributes zero to the sum.

• let $z = \frac{b+c}{b} \mod p$.

• There is a unique integer z, $0 \le z \le p-1$, for each b.

• $1 \le b \le p-1 \Rightarrow$ z takes on the values $0, 2, \dots, p-1$, but not 1 (as $c \not\equiv 0 \mod p$)

$$\therefore \sum_{b=0}^{p-1} \chi(b)\chi(b+c) = \sum_{b=1}^{p-1} \chi(b)\chi(bz)$$

$$= \sum_{b=1}^{p-1} (\chi(b))^2 \chi(z) \quad [\because \chi(b)^2 = 1]$$

$$= \sum_{\substack{z=0 \\ z \ne 1}}^{p-1} \chi(z)$$

$$= \sum_{z=1}^{p-1} \chi(z) - \chi(1) \quad [\chi(0) = 0]$$

half $+1$, half -1

$$= 0 - \chi(1)$$

$$= -1. \quad [1^2 \equiv 1 \mod p \Rightarrow \chi(1) = 1.]$$

~~Very similar properties hold~~

• $\chi(i) \equiv i^{\frac{p-1}{2}} \pmod p$ (Euler's criterion)

• $\chi(-1) \equiv (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{cases}$

± 1 $\quad$ ± 1

$\chi(-1) - (-1)^{\frac{p-1}{2}} \to 0$ or $\cancel{2} \mod p$

Claim $A(n,d) = 2\left\lfloor \frac{d}{2d-n} \right\rfloor$ if $2d > n \geq d$.

$QR_7 = \{1, 4, 2\}$, $QNR_7 = \{3, 5, 6\}$.

Example: $p = 7 = 4\times1+3$

Jacobsthal matrix $Q = (q_{ij})_{p\times p}$, $q_{ij} = \chi(j-i)$

$$Q = \begin{array}{c|ccccccc|} & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 0 & 0 & 1 & 1 & - & 1 & - & - \\ 1 & - & 0 & 1 & 1 & - & 1 & - \\ 2 & - & - & 0 & 1 & 1 & - & 1 \\ 3 & 1 & - & - & 0 & 1 & 1 & - \\ 4 & - & 1 & - & - & 0 & 1 & 1 \\ 5 & 1 & - & 1 & - & - & 0 & 1 \\ 6 & 1 & 1 & - & 1 & - & - & 0 \end{array}$$

$i \downarrow$, $j \rightarrow$

- $q_{ji} = \chi(i-j)$
  $= \chi(-1)\chi(j-i)$
  $= -q_{ij}$
- $-1 \in QNR$.
- if $p = 4k+1$, $\chi(-1) = 1$
- if $p = 4k+3$, $\chi(-1) = -1$.

- Q is skew symmetric i.e. $Q^T = -Q$.

Lemma $QQ^T = pI - J$, and $QJ = JQ = 0$, where J is the matrix of order p all of whose entries are 1

proof let $P = (p_{ij}) = QQ^T$

$$\therefore p_{ii} = \sum_{k=0}^{p-1} q_{ik}^2 = p-1$$

$$p_{ij} = \sum_{k=0}^{p-1} q_{ik}q_{jk} = \sum_{k=0}^{p-1} \chi(k-i)\chi(k-j), \ i \neq j$$

$$= \sum_{k=0}^{p-1} \chi(b)\chi(b+c), \ c \neq 0 \bmod p$$

$$= -1$$

$k-i = b$
$k-j = k-i+i-j = b+c$
$c = i-j \neq 0 \bmod p$

$A = (a_{ij})_{n\times n}$
$B = (b_{ij})_{n\times n}$
$AB = (c_{ij})$
$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$, $b_{kj} \to a_{jk}$

$$\therefore QQ^T = \begin{pmatrix} p-1 & & -1 \\ & p-1 & \\ -1 & & p-1 \end{pmatrix}_{p\times p} + J - J = pI_{p\times p} - J$$

$QJ = JQ = 0$ as each row & column of Q contains $\frac{p-1}{2}$ $+1$'s & $\frac{p-1}{2}$ -1's.

row sum column sum.

Paley type Hadamard matrix

Let $\underset{(p+1)\times(p+1)}{H} = \begin{pmatrix} 1 & 1 \\ 1^T & Q-I \end{pmatrix}$, then $HH^T = (p+1) I_{p+1}$.

~~$HH^T = (p+1)\times(p+1)$.~~

proof

$$\underset{p+1\times p+1}{HH^T} = \begin{pmatrix} 1 & 1 \\ 1^T & Q-I_p \end{pmatrix} \begin{pmatrix} 1 & \overbrace{1}^{p \text{ columns}} \\ 1^T & Q^T - I_p \end{pmatrix}$$

makes diagonal of Q^T all -1

each row having $\frac{p-1}{2}$ $+1$'s, $\frac{p-1}{2}$ -1's

$$= \begin{pmatrix} p+1 & 0 \\ 0 & J + (Q-I_p)(Q^T - I_p) \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}_{n\times 1} \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}_{1\times n} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \end{pmatrix}_{n\times n} = J.$$

$J + (Q - I_p)(Q^T - I_p)$

$= J + QQ^T - Q - Q^T + I_p$

$= \cancel{J} + pI_p - \cancel{J} - \cancel{Q} - \cancel{Q^T} + I_p$

$= (p+1) I_p$.

$$\therefore HH^T = \begin{pmatrix} p+1 & 0 \\ 0 & (p+1)I_p \end{pmatrix} = (p+1) I_{p+1}.$$

- Construction I (Sylvester type) $\hookrightarrow n = 2^r$ multiple of 4 & Construction II (Paley type) $n = 2p+1$ mul. of 4 together give Hadamard matrices of all orders 1, 2, 4, 8, 12, ..., 32.

- Equivalent Hadamard matrices

$$H_k \equiv H_l \quad \text{iff} \quad H_k \xrightarrow[\text{column permutation}]{\text{(i) row or}} H_l$$

(ii) multiplying rows/columns by -1.

$$\left(\begin{array}{c} R_i \Leftrightarrow R_j \\ C_i \Leftrightarrow C_j \\ -R_i \\ -C_i \end{array} \right)$$

1) 1 equivalence class of Hadamard matrices of orders 1, 2 and 4

2) 1 equivalence class of order 8.

3) 1 equivalence class of order 12

4) 5 equivalence classes of order 16

5) 3 equivalence classes of order 20.

6) # equivalence classes of order 24 $\rightarrow$ unknown.

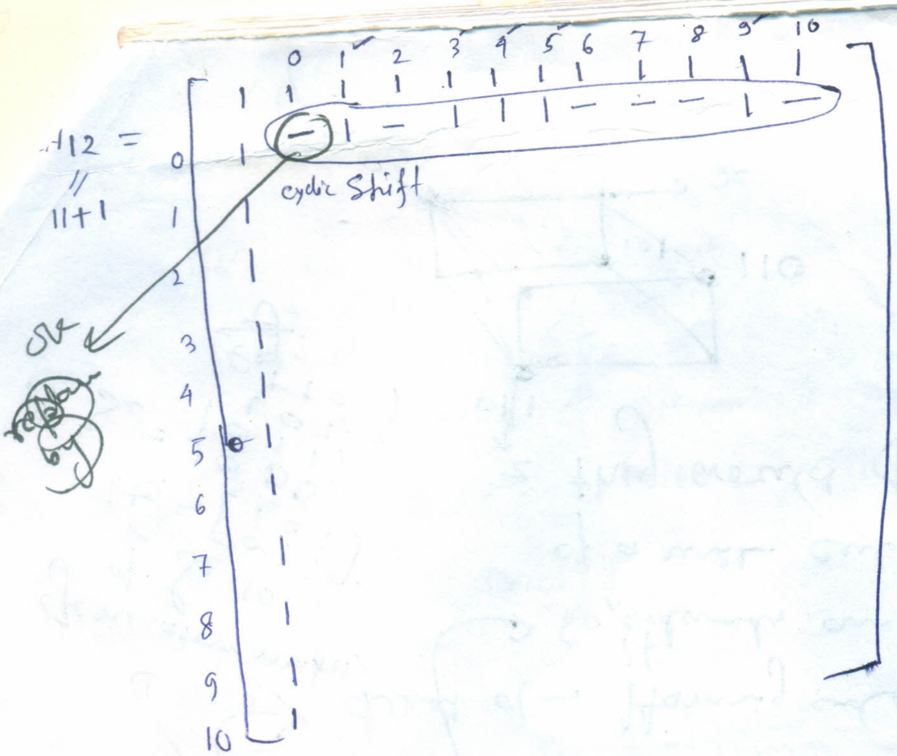
$QR_7 = \{1, 4, 2\}$

- $H_8 =$ Sylvester type

$$H_8 = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array} \right)$$

$H_8 =$ 7+1

$$\begin{array}{c} \\ \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \left(\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{array} \right) \end{array}$$



$QR_{11} = \{1, 4, 9, 5, 3\}$

$\frac{n}{2}$ +1's → A_n → $\frac{n}{2}$ 0's, $\frac{n}{2}$ 1's

$\frac{n}{2}$ −1's. each row has $\frac{n}{2}$ +1's.

$$H_n = \begin{pmatrix} 1 & 1 \\ 1^T & Q-I \end{pmatrix}$$

$Q_{n-1} = \begin{pmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{pmatrix}$, QR +1, QNR −1

$Q - I = \begin{pmatrix} -1 & & \\ & -1 & \\ & & \ddots \\ & & & -1 \end{pmatrix}$

Hadamard Codes

- H_n → normalized Hadamard matrix of order n.
  - → replace +1's by ~~1's~~ 0's
  - & −1's by +1's.
- A_n → binary Hadamard matrix ~~A_n~~.
  - → two rows of A_n agree in $\frac{1}{2}n$ places & differ in $\frac{1}{2}n$ places (as rows of H_n are orthogonal)
  - → two rows of A_n are $\frac{1}{2}n$ Hamming distance apart.

each row

- A_n gives rise to 3 Hadamard codes:

(i) delete first column of A_n → rows of A_n are codewords with 1st column deleted.

$\mathcal{A}_n$ $(n-1, n, \frac{1}{2}n)$ Hadamard code

(ii) augment $\mathcal{A}_n$ i.e. $\mathcal{A}_n \cup \{1+\mathcal{A}_n\}$.

$\mathcal{B}_n$ $(n-1, 2n, \frac{1}{2}n-1)$ Hadamard code

$d^{(a)} = \min(d, n-1-d')$

d' = largest wt. of a codeword in $= \frac{1}{2}n$

(iii) augment A_n i.e. $A_n \cup \{1+A_n\}$

$\mathcal{C}_n$ $(n, 2n, \frac{1}{2}n)$ Hadamard code

- A_n is a simplex code as distance between two codewords is $\frac{1}{2}n$
- H_n with $n = 2^r$ (Sylvester type) generates linear codes A_n, ~~$\mathcal{B}_n$~~, B_n & C_n.
- A_n, B_n, C_n are non-linear if underlying H_n is of Paley type Hadamard matrix for $n > 8$.

$\rightarrow$ linear span of these codes generate linear codes, called <u>quadratic residue codes</u>

- Other construction of H_n also possible, but in that case binary rank of A_n very little is known about the

$H_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ $3, 1$ $r = 2$

$\mathcal{H}_r \rightarrow [2^r - 1, 2^r - 1 - r]$

$S_r \rightarrow [2^r - 1, r]$

generator matrix of $\mathcal{H}_r$ is 1×3 $= [1\,1\,1]$

- Simplex code $\rightarrow$ every pair of codewords is the same distance apart.

$\mathcal{H}_2 = \begin{Bmatrix} 000, \\ 111 \end{Bmatrix}$

$\rightarrow$ dual of Hamming code.

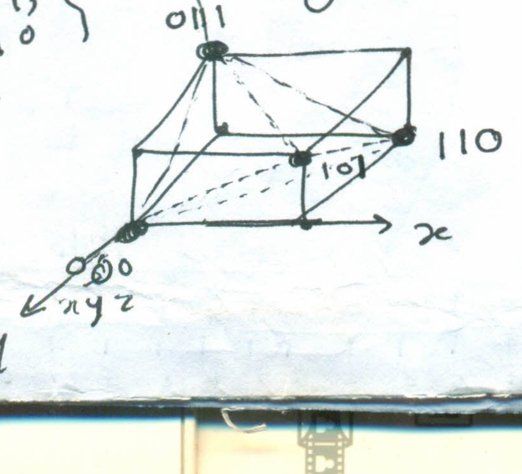
$\rightarrow$ So, if codewords are marked at the vertices of a unit cube in n dimensions, they would form a regular simplex.

generator matrix of S_2 is

$H_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

$\therefore S_2 = \{000, 011, 101, 110\}$

eg.



$S_2 = \begin{Bmatrix} 000, \\ 011, \\ 101, \\ 110 \end{Bmatrix}$

$\rightarrow$ forms a regular tetrahedron.

Conference (C-) Matrices

- Similar to Hadamard matrices
  ↓ gives
- good non-linear codes
- used in the design of networks having same attenuation between every pair of terminals.
- $C_{n\times n}$ → diagonal entries 0, other entries +1, −1 s.t.

$$C_{n\times n} C^T = (n-1) I_n$$

Properties

1. Normalized C-matrices

$$C = \begin{pmatrix} 0 & 1 \\ 1^T & S \end{pmatrix}, \quad S_{(n-1)\times(n-1)} \text{ matrix s.t.}$$

$$SS^T = (n-1)I_{n-1} - J_{n-1}$$

$$SJ = JS = 0.$$

$$C_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & - \\ 1 & - & 0 & 1 \\ 1 & 1 & - & 0 \end{pmatrix}$$

n must be even.

2. if C exists, then
   - if $n \equiv 2 \pmod 4$ then C can be made symm.
   - if $n \equiv 0 \pmod 4$ then C can be made skew-symm

3. • Conversely, if a symm. C exists, then $n \equiv 2 \pmod 4$ & n−1 can be written as $n-1 = a^2+b^2$

   where a, b are integers.

   • if a skew-symm C exists, then $n = 2$ or $n \equiv 0 \pmod 4$

Several constructions

(Paley):

- $n = p^m + 1 \equiv 2 \pmod 4$, p odd prime
- $p^m \times p^m$ Jacobsthal matrix $Q = (q_{ij})$, $q_{ij} = \chi(j-i)$
- $p^m \equiv 1 \pmod 4$, so Q symm.

Set $C = \begin{pmatrix} 0 & 1 \\ 1^T & Q \end{pmatrix} \rightarrow$ a symm. conference matrix of order n.

Example: $n = 6$, $p^m = 5$. $\qquad QR_5 = \{1, 4\}$

$$C_6 = \begin{array}{c|c} & \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} & \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{array}\right] \end{array}$$

Codes from Conference matrices

- $C_n \rightarrow$ symm. conference matrix

$n \equiv 2 \pmod 4$

- rows of

$\frac{1}{2}(S + I + J)$ → diagonal → all 1's, 1's → 1's, −1's → 0's.

$\frac{1}{2}(-S + I + J)$ → diagonal → all 1's, 1's → 0's, −1's → 1's

all-zero vector

all-one vector

$\rightarrow (n-1, 2n, \frac{1}{2}(n-2))$ ← why?

Conference matrix code.

$(n-1) - \left(\frac{n-2}{2} + 1\right) = \frac{n-2}{2}$

$\frac{n-2}{2}$ $\quad n - \frac{n-2}{2} + 1 = n - \frac{n+2}{2}$

each row → $\left(\frac{n-2}{2} + 1\right)$ 1's.

~~two rows differ in~~ → ~~$\frac{n-1}{2}$ places~~

min ~~weight~~ wt. of any column → $\frac{n-2}{2} + 1$

Conference Matrix. C_{10}

- $n = 10 = 3^2 + 1$
- $GF(3^2)$ generated by $\alpha^2 + \alpha + 2 = 0$.

	elements		binary	~~powers of α~~
$GF(3^2)$ elements.	0	$-$	$0\ 0$	
	α	α	$0\ 1$	
	2α	α^5	$0\ 2$	
	1	α^8	$1\ 0$	
	$1+\alpha$	α^7	$1\ 1$	
	$1+2\alpha$	α^2	$1\ 2$	
	2	α^4	$2\ 0$	
	$2+\alpha$	α^6	$2\ 1$	
	$2+2\alpha$.	α^3	$2\ 2$	

QRs modulo 9 $\longrightarrow$ $\boxed{1,\ \alpha^2 = 2\alpha+1,\ \alpha^4 = 2,\ \alpha+2}$

$\alpha^2 = 2\alpha+1$

$(2\alpha)^2 = 4\alpha^2 = \alpha^2 = -\alpha-2 = 2\alpha+1$

$1^2 = 1$

$(1+\alpha)^2 = 1+2\alpha+\alpha^2 = 1+2\alpha-\alpha-2 = \alpha-1 = \alpha+2$

$(1+2\alpha)^2 = 1+4\alpha+4\alpha^2 = 1+\alpha+\alpha^2 = 1+\cancel{\alpha}-\cancel{\alpha}-2 = -1 = 2$

$\alpha \to 01$

$\alpha^2 = -\alpha-2 = 2\alpha+1 \to 12$

$\alpha^3 = -\alpha^2-2\alpha = \alpha+2-2\alpha = 2-\alpha = 2+2\alpha \to 22$

$\alpha^4 = 2\alpha+2\alpha^2 = 2\cancel{\alpha}+2(\cancel{-\alpha}-2) = -4 = -1 = 2 \to 20$

$\alpha^5 = 2\alpha \to 02$

$\alpha^6 = 2\alpha^2 = 2(-\alpha-2) = -2\alpha-4 = \alpha-1 = \alpha+2 \to 21$

$\alpha^7 = \alpha^2+2\alpha = -\alpha-2+2\alpha = \alpha-2 = \alpha+1 \to 11$

$\alpha^8 = \alpha^2+\alpha = -\cancel{\alpha}-2+\cancel{\alpha} = -2 = 1 \to 01$

$$C_{10} = \begin{array}{c|cccccccccc}
 & & 0 & 1 & 2 & \alpha & \alpha+1 & \alpha+2 & 2\alpha & 2\alpha+1 & 2\alpha+2 \\
\hline
 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & - & - & 1 & - & 1 & - \\
1 & 1 & 1 & 0 & 1 & 1 & - & - & 1 & - & 1 \\
\alpha & 1 & & & 0 & & & & & & \\
\alpha+1 & 1 & & & & 0 & & & & & \\
\alpha+2 & 1 & & & & & 0 & & & & \\
2\alpha & 1 & & & & & & 0 & & & \\
2\alpha+1 & 1 & & & & & & & 0 & & \\
2\alpha+2 & 1 & & & & & & & & 0 & \\
 & 1 & & & & & & & & & 0
\end{array}$$

$\alpha^2 = -\alpha-2$
$= 2\alpha+1$

$\alpha^3 = 2\alpha^2+\alpha$
$= -2\alpha-4+\alpha$
$= \alpha+2+\alpha$
$= 2\alpha+2$

$\alpha^4 = 2\alpha^2+2\alpha$
$= -2\cancel{\alpha}-4+2\cancel{\alpha}$
$= -1 = 2$

$\alpha^5 = 2\alpha$

$\alpha^6 = 2\alpha^2 = -2\alpha-4$
$= \alpha+2$

$\alpha^7 = \alpha^2+\alpha$
$= -\cancel{\alpha}-2+\cancel{\alpha}$
$= 1$

$\alpha^8 = \alpha$

$(2\alpha)^2 = 4\alpha^2 = \alpha^2 = -\alpha-2$

$(1+\alpha)^2 = 1+2\alpha+\alpha^2$
$= 1+2\alpha-\alpha-2$
$= -1+\alpha = 2+\alpha$

$(\alpha+2)^2 = \alpha^2+4\alpha+4$
$= \alpha^2+\alpha+1$
$= -\alpha-2+\alpha+1$
$= -1 = 2$

$2+\alpha = -\alpha^2$
$= 2\alpha^2$

$\alpha^8 = 1.$

~~$\alpha(\alpha-1) = \alpha^2$~~

$\alpha-1 = \alpha+2$

$\alpha^2+\alpha+2=0$
$GF(3^2)$

$$C_{10} = \begin{array}{c} \\ \\ 0 \\ 1 \\ 2 \\ \alpha \\ \alpha+1 \\ \alpha+2 \\ 2\alpha \\ 2\alpha+1 \\ 2\alpha+2 \end{array}
\begin{array}{cccccccccc}
 & 0 & 1 & 2 & \alpha & \alpha+1 & \alpha+2 & 2\alpha & 2\alpha+1 & 2\alpha+2 \\
\end{array}$$

$$C_{10} = \begin{array}{c|cccccccccc}
 & & 0 & 1 & 2 & \alpha & \alpha+1 & \alpha+2 & 2\alpha & 2\alpha+1 & 2\alpha+2 \\
\hline
 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & - & - & 1 & - & 1 & - \\
1 & 1 & 1 & 0 & 1 & 1 & - & - & - & - & 1 \\
2 & 1 & 1 & 1 & 0 & - & 1 & - & 1 & - & - \\
\alpha & 1 & - & 1 & - & 0 & 1 & 1 & - & - & 1 \\
\alpha+1 & 1 & - & - & 1 & 1 & 0 & 1 & 1 & - & - \\
\alpha+2 & 1 & 1 & - & - & 1 & 1 & 0 & - & 1 & - \\
2\alpha & 1 & - & - & 1 & - & 1 & - & 0 & 1 & 1 \\
2\alpha+1 & 1 & 1 & - & - & - & - & 1 & 1 & 0 & 1 \\
2\alpha+2 & 1 & - & 1 & - & 1 & - & - & 1 & 1 & 0
\end{array}$$

$\alpha-1=\alpha+2$
$\alpha+1-1=\alpha$
$\alpha+2-1=\alpha+1$
$2\alpha-1=2\alpha+2$
$2\alpha+1-1=2\alpha$
$2\alpha+2-1=2\alpha+1$

$0-2=1$
$1-2=-1$
$\alpha-2=\alpha+1$
$\alpha+1-2=\alpha-1$
$=\alpha+2$

$\alpha+\cancel{2}-\cancel{2}$
$2\alpha-2=2\alpha+1$
$2\alpha+1-2=2\alpha-1$
$=2\alpha+2$
$2\alpha+2-2=2\alpha$

$\underbrace{\qquad\qquad}_{S}$

Symm., but 2^{nd} row is not the right cyclic shift of 1st. row.

Conference code $\quad (n-1,\ 2n,\ \frac{1}{2}(n-2))$ code.

$\frac{1}{2}(S+I+J)$, $\frac{1}{2}(-S+I+J)$, $\underbrace{00\cdots0}_{n-1}$, $\underbrace{11\cdots1}_{n-1}$

- diagonal entries all 1

$\frac{1}{2}(S+I+J)$:
- +1's of S remains +1
- −1's of S becomes 0

$\frac{1}{2}(-S+I+J)$:
- +1's of S becomes 0
- −1's of S becomes 1

- $H_n \to A_n$
  replace -1's by $+1$'s & $+1$'s by 0's.

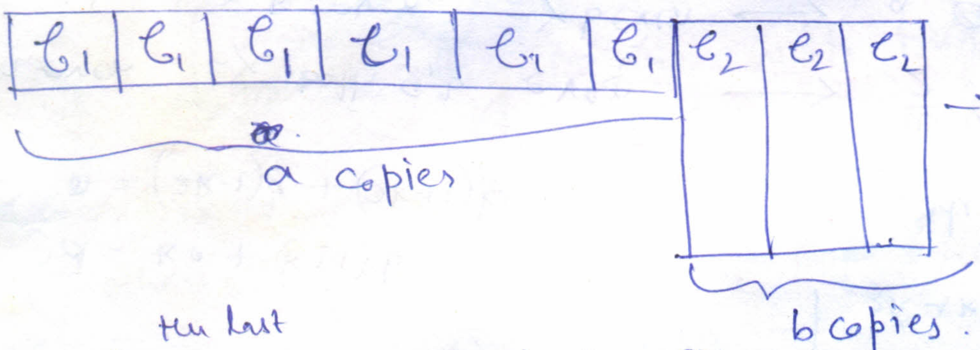
$\to \mathcal{A}_n$ (1st. column of A_n deleted) $\quad (n-1, n, \frac{1}{2}n)$

$\to \mathcal{B}_n = \mathcal{A}_n \cup (1+\mathcal{A}_n) \quad (n-1, 2n, \frac{1}{2}n-1)$

$\to \mathcal{C}_n = A_n \cup (1+A_n). \quad (n, 2n, \frac{1}{2}n)$

- Codewords of $\mathcal{A}_n$ that begin with $0 \to$ delete initial zero
  $\downarrow$
  $\mathcal{A}_n' \quad (n-2, \frac{n}{2}, \frac{n}{2})$.

- $\mathcal{C}_1(n_1, M_1, d_1)$, $\mathcal{C}_2(n_2, M_2, d_2)$.



$\mathcal{C} = a\mathcal{C}_1 \oplus b\mathcal{C}_2$

$\to (n, M, d)$

$n = an_1 + bn_2$
$M = \min\{M_1, M_2\}$.
$d \geq ad_1 + bd_2$

- omit the last $M_2 - M_1$ rows of $\mathcal{C}_2$ (if $M_2 > M_1$)
- omit the last $M_1 - M_2$ rows of $\mathcal{C}_1$ (if $M_1 > M_2$).

Levensthein Theorem

Provided enough Hadamard matrices exist, equality holds in the Plotkin bound.

- if d is even, $\quad A(n,d) = 2\left\lfloor \frac{d}{2d-n} \right\rfloor$ if $2d > n \geq d$ — ①

  $A(2d, d) = 4d$ — ②

- if d is odd, $\quad A(n,d) = 2\left\lfloor \frac{d+1}{2d+1-n} \right\rfloor$ if $2d+1 > n \geq d$ — ③

  $A(2d+1, d) = 4d+4$ — ④.

Proof. $\underline{d \text{ even}}$ $\quad$ (③, ④ follows from $A(n, 2r-1) = A(n+1, 2r)$)

② follows as $\mathcal{C}_{..}$ is an $(2d, 4d, d)$ code.

Claim $A(n,d) = 2\left\lfloor \frac{d}{2d-n} \right\rfloor$ if $2d > n \geq d$.

Construction of (n, M, d) Code with $M = 2\left\lfloor \frac{d}{2d-n} \right\rfloor$

- $2d > n \geq d$
- $k = \left\lfloor \frac{d}{2d-n} \right\rfloor$
- $\left.\begin{array}{l} a = d(2k+1) - n(k+1) \\ b = -d(2k-1) + kn \end{array}\right\}$ a,b non negative integers (~~proof~~ ~~omitted~~)

$$\frac{d}{b(k+1)+ak} = \frac{n}{a(2k-1)+b(2k+1)} = \frac{1}{k(2k+1) - (k+1)(2k-1)}$$

$d(2k+1) - n(k+1) - a = 0$

$-d(2k-1) + nk - b = 0$

$\cancel{2k^2} + k - (\cancel{2k^2} - k + 2k - 1)$

- $d = ka + (k+1)b$

$n = (2k-1)a + (2k+1)b$.

Code $\mathcal{C}(n, M, d)$

- n even $\Rightarrow$ both a, b even $\longrightarrow \frac{a}{2}A'_{4k} \oplus \frac{b}{2}A'_{4k+4}$
- n odd
  - $\longrightarrow k$ even $\Rightarrow b$ even $\longrightarrow a A_{2k} \oplus \frac{b}{2}A'_{4k+4}$
  - $\longrightarrow k$ odd. $\Rightarrow a$ even $\longrightarrow \frac{a}{2}A'_{4k} \oplus b A_{2k+2}$

Check.

$\frac{a}{2}A'_{4k} \oplus \frac{b}{2}A'_{4k+4}$

$\downarrow$

$A'_n\left(n-2, \frac{n}{2}, \frac{n}{2}\right)$

$\longrightarrow \tilde{n} = \frac{a}{2}n_1 + \frac{b}{2}n_2 = \frac{a}{2}(4k-2) + \frac{b}{2}(4k+4-2) = n$

$\longrightarrow \tilde{M} = \min\left(\frac{4k}{2}, \frac{4k+4}{2}\right) = 2k = M$

$\longrightarrow \tilde{d} \geq \frac{a}{2}\cdot\frac{4k}{2} + \frac{b}{2}\cdot\frac{4k+4}{2} = d$.

$a A_{2k} \oplus \frac{b}{2}A'_{4k+4}$

$\downarrow$

$A_n\left(n-1, n, \frac{n}{2}\right)$

$\longrightarrow \tilde{n} = \frac{a}{2}d_1 + \frac{b}{2}d_2 = a\cdot(2k-1) + \frac{b}{2}\cdot(4k+4-2) = n$

$\longrightarrow \tilde{M} = \min\left\{2k, \frac{4k+4}{2}\right\} = 2k = M$

$\longrightarrow \tilde{d} \geq a\cdot\frac{2k}{2} + \frac{b}{2}\cdot\frac{4k+4}{2} = d$

$\frac{a}{2}A'_{4k} \oplus b A_{2k+2}$

$\longrightarrow \frac{a}{2}\cdot(4k-2) + b\cdot(2k+2-1) = n$

$\longrightarrow \tilde{M} = \min\left\{\frac{4k}{2}, \frac{2k+2}{2}\right\} = 2k = M$

$\longrightarrow \tilde{d} \geq \frac{a}{2}\cdot\frac{4k}{2} + b\cdot\frac{2k+2}{2} = d$