Linear Block Codes

- Given a finite field *GF(q)* : Galois Field

$$\text{let } GF(q)^n = \{\underline{x} \mid \underline{x} = (x_1, x_2, \ldots, x_n), x_i \in GF(q)\}$$
$$\forall \underline{x}, \underline{y} \in GF(q)^n, a \in GF(q) \quad \text{s.t.}$$
$$\underline{x} + \underline{y} \equiv (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \in GF(q)^n$$
$$a \cdot \underline{x} \equiv (a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n) \in GF(q)^n$$
$$\Rightarrow GF(q)^n \text{ is a vector space}$$

- Definition : An linear code ***C*** = (n,k) is a k-dimensional subspace of *GF(q)*^{n}, i.e.

$$\begin{cases} (1) \forall \underline{x}, \underline{y} \in C, \underline{x} + \underline{y} \in C, \\ (2) \forall a \in GF(q) \text{ and } \underline{x} \in C, a \cdot \underline{x} \in C, \text{and} \end{cases}$$
$$(3)\ \underline{0} \in C.$$

* (3) 可由(2)推得!

Definition : Hamming distance d($\underline{x}$,$\underline{y}$) is the number of places in which they differ.

$x = (x_1, x_2, x_3)$
$y = (y_1, y_2, y_3)$

Proof (problem 3.7):

Let x, y and z be any three *n*-tuples over GF(2). Note that

d(x,y) = *w*(x + y);

d(y,z) = *w*(y + z);

d(x,z) = *w*(x + z):

It is easy to see that

w(u) + *w*(v) >= *w*(u + v) ..... (1)

Let u = x + y and v = y + z. It follows from (1) that

w(x + y) + *w*(y + z) >= *w*(x + y + y + z) = *w*(x + z):

From the above inequality, we have

d(x; y) + *d*(y; z) > =*d*(x; z):

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

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

$\mathbb{R}^3 \quad d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2}$

$[GF(2)]^3$

Definition : minimum distance of C is the hamming distance of the pair of codewords with smallest hamming distance, ie $d^* = \min d(\underline{x}_i,\underline{x}_j)$, $\underline{x}_i,\underline{x}_j \in C$, $i \neq j$.

Definition : The Hamming weight $W(c)$ of a codeword c is equal to the number of nonzero components in the codeword. The minimum weight W^* of a code is the smallest weight of nonzero codeword.

Theorem : $d^* = \min_{c\neq 0} W(c) = W^*$

Proof: $$d^* = \min_{c_i,c_j\in C, i\neq j} d(c_i,c_j)$$

$$\because \quad = \min_{c_i,c_j\in C, i\neq j} d(0, c_i - c_j) = \min_{c\in C, c\neq 0} W(c) = W^*$$

linear $\quad C^{16}_2 \quad c \neq 0 \quad$ 15 种

$GH^T = 0$

TABLE 1. LINEAR BLOCK CODE WITH k = 4 AND n = 7 $d^*=3$ $\parallel$ W^*

$v = u \cdot G$

Messages (u)		Code words	
(0 0 0 0)		(0 0 0 0 0 0 0)	
(1 0 0 0)	v	(1 1 0 1 0 0 0)	g_0
(0 1 0 0)	v	(0 1 1 0 1 0 0)	g_1
(1 1 0 0)		(1 0 1 1 1 0 0)	
(0 0 1 0)	v	(1 1 1 0 0 1 0)	g_2
(1 0 1 0)		(0 0 1 1 0 1 0)	
(0 1 1 0)		(1 0 0 0 1 1 0)	
(1 1 1 0)		(0 1 0 1 1 1 0)	
(0 0 0 1)	v	(1 0 1 0 0 0 1)	g_3
(1 0 0 1)		(0 1 1 1 0 0 1)	
(0 1 0 1)		(1 1 0 0 1 0 1)	
u = (1 1 0 1)	v =	(0 0 0 1 1 0 1)	
(0 0 1 1)		(0 1 0 0 0 1 1)	
(1 0 1 1)		(1 0 0 1 0 1 1)	
(0 1 1 1)		(0 0 1 0 1 1 1)	
(1 1 1 1)		(1 1 1 1 1 1 1)	

parity-check $\quad$ information

$$G = \begin{pmatrix} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 1&1&1&0&0&1&0 \\ 1&0&1&0&0&0&1 \end{pmatrix}_{4\times 7}$$

$GH' = 0$

$$H = \begin{pmatrix} 1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{pmatrix}_{3\times 7}$$

$H' = H^T$

$v = 1\cdot g_0 + 1\cdot g_1 + 0\cdot g_2 + 1\cdot g_3$

Q :
1. 想想 parity-check bits 形成機制？
2. (7,4) block codes 有幾組? (i.e. 有幾個 dim=4之 subspace)

Matrix Discription of Linear Block Codes (n,k)

$\cancel{v = u \times G}$

1xn   1xk   kxn

$\cancel{= (u_0, u_1, \ldots, u_{k-1})} \times \begin{pmatrix} g_0 \\ g_1 \\ \cdot \\ \cdot \\ \cdot \\ g_{k-1} \end{pmatrix}$ K linear independent basis code words

Q:如何找?

$a\cdot(1\ 0\ 1)$
$+b\ (0,1,0)$
$=(0,0,0)$
$\Rightarrow a=b=0$
(a,b,a)

$= u_0 g_0 + u_1 g_1 + \ldots + u_{k-1} g_{k-1}$

$= (v_0, v_1, \ldots, v_{n-1})$

$$G = \begin{pmatrix} \mathbf{g_0} \\ \mathbf{g_1} \\ \cdot \\ \cdot \\ \cdot \\ \mathbf{g_{k-1}} \end{pmatrix} = \begin{pmatrix} g_{00} & g_{01} & g_{02} & \ldots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \ldots & g_{1,n-1} \\ \circ & & \circ & & \circ \\ \circ & & \circ & & \circ \\ \circ & & \circ & & \circ \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \ldots & g_{k-1,n-1} \end{pmatrix}_{k \times n}$$

generator matrix

where $\mathbf{g}_i = (g_{i0}, g_{i1}, \ldots, g_{i,n-1})$ for $0 \le i < k$.

$\rightarrow$(n,k) linear code is completely specified by the k rows of G

$r = v + e$

$v=(0\ 0\ 0\ 0\ 0\ 0\ 0)$
$e=(0\ 1\ 0\ 0\ 0\ 0\ 0)$
$r=(0\ 1\ 0\ 0\ 0\ 0\ 0)$

Goal :

Looking for H = ?

s.t. $rH^T = vH^T + eH^T$ & $vH^T = 0$

$\therefore$ if $GH^T = 0_{k\times(n-k)}$ then $vH^T = u \times GH^T = 0$

$G \cdot H^T = 0$

$(\ \ )_{k\times k} \cong (\ \ ) \to I_k$

Code (= u×G): row space of G

Q1 : By 1. elementary row operations
2. column permutation

$$G = \begin{pmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \cdot \\ \cdot \\ \cdot \\ \mathbf{g}_{k-1} \end{pmatrix} = \underbrace{\begin{pmatrix} p_{00} & p_{01} & \ldots & p_{0,n-k-1} \\ p_{10} & p_{11} & \ldots & p_{1,n-k-1} \\ & & & \\ p_{k-1,0} & p_{k-1,1} & \ldots & p_{k-1,n-k-1} \end{pmatrix}}_{\text{P matrix}} \underbrace{\begin{matrix} 1\ 0\ 0 \ldots 0 \\ 0\ 1\ 0 \ldots 0 \\ \\ 0\ 0\ 0 \ldots 1 \end{matrix}}_{\text{k x k identity matrix}}{}_{k \times n} = [\mathbf{P}\ \mathbf{I}_k]$$

Q2: 作 COLUMN PERMUTATION, G之ROW SPACE不會改變嗎?

$$\mathbf{H} = [\ \mathbf{I}_{n-k}\ \mathbf{P}^T\ ]$$

Q : $GH^T = 0$

parity-check matrix

$$= \begin{pmatrix} 1\ 0\ 0 \ldots 0 & p_{00} & p_{10} & \ldots & p_{k-1,0} \\ 0\ 1\ 0 \ldots 0 & p_{01} & p_{11} & \ldots & p_{k-1,1} \\ 0\ 0\ 1 \ldots 0 & p_{02} & p_{12} & \ldots & p_{k-1,2} \\ \circ & & & & \\ \circ & & & & \\ \circ & & & & \\ 0\ 0\ 0 \ldots 1 & p_{0,n-k-1} & p_{1,n-k-1} & \ldots & p_{k-1,n-k-1} \end{pmatrix}_{(n-k) \times n}$$

Theorem 1 : An n-tuple v is a codeword in the code generated by G iff $v \cdot H^T = 0$ ← parity checking equation

Q : prove it (←) see next page

- G $\longleftrightarrow$ code C : (n, k)
  H $\longleftrightarrow$ dual code of C (C_d: (n, n-k)):
  H^T : the null space of G (i.e. $GH^T=0$)

- From G ($v = u \times G$) $1\times n \quad 1\times k \quad k\times n$
  $v_{n-k+i} = u_i,\ 0 \le i \le k-1$
  $v_j = u_0 p_{0j} + u_1 p_{1j} + \ldots + u_{k-1} p_{k-1\,j},\ 0 \le j \le n-k-1$

- From H ($vH^T = 0$)
  $v_j + u_0 p_{0j} + u_1 p_{1j} + \ldots + u_{k-1} p_{k-1\,j} = 0,\ 0 \le j \le n-k-1$
  $(v = (\underline{v_0, v_1, \ldots, v_{n-k-1}}, \underline{u_0, u_1, \ldots, u_{k-1}})$

Q : physical meaning

➔ (n,k) linear code is completely specified by H

Theorem 2 : Every linear code ≈ a systematic linear code

Q : 有幾種 (n, k) linear block codes ?

$1\times n \quad n\times n-k$

Error-Detecting & Error-Correcting Capability

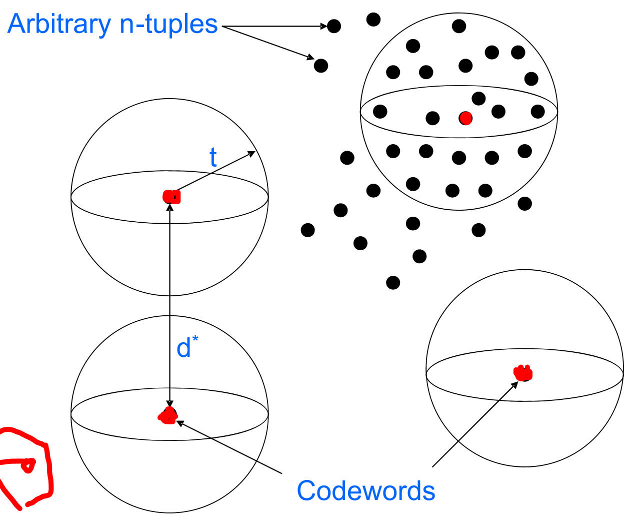


Figure 1. Decoding spheres

$v=(v_0,\ldots,v_{n-1})$ transmitted codeword
$r=(r_0,\ldots,r_{n-1})$ received vector
$e=(e_0,\ldots,e_{n-1})$ error pattern
➔ $r = v + e$
➔ $s = r \cdot H^T = eH^T$ $\quad vH^T=0$
└ syndrome of r

\# s=0 iff r is a codeword
\# undetectable error pattern (2^k-1)
detectable error pattern
($2^n-1-(2^k-1) = 2^n-2^k$)

$r = v + e$

Example. (7,4) block code

$rH^T = 0$

A_i : # of code vector of weight i in C

if $r \in C$ then $e \in C$

$P_u(E) = \sum_{i=1}^{n} A_i P^i (1-p)^{n-i} \Rightarrow$ Prob. of undetected error

$A_0=1\ A_1=A_2=0\ A_3=7\ A_4=7\ A_5=A_6=0\ A_7=1$

if $p=10^{-2}$ $p_u(e) \approx 7 \times 10^{-6}$

eH^T

n-k

$$S_0=e_0+e_{n-k}p_{00}+e_{n-k+1}p_{10}+\ldots+e_{n-1}p_{k-1,0}$$
$$S_1=e_1+e_{n-k}p_{01}+e_{n-k+1}p_{11}+\ldots+e_{n-1}p_{k-1,1}$$
$$\vdots$$
$$S_{n-k-1}=e_{n-k-1}+e_{n-k}p_{0,n-k-1}+\ldots+e_{n-1}p_{k-1,\ n-k-1}$$

$\shortparallel$

$(e_0\ e_1 \cdots e_{n-1})$

Theorem 3 : t-error detecting iff $d^* \geq t+1$

t-error correcting iff $d^* \geq 2t+1$

- incomplete decoder & complete decoder
- Perfect code --- e.g. Hamming code

n-k linear equation
It has 2^k solutions
Prove it!
(Thm. 3.6)

t-error correcting iff $d^* \geq 2t+1$

Pf: $\Leftarrow$

(i) (> t errors)

$2t+1 \leq d^* \leq 2t+2$

let $d(\mathbf{v},\mathbf{w}) = d^*$

$\mathbf{v}+\mathbf{w} = \mathbf{a}$ = (XXX…X ΔΔ…Δ)

取 $\mathbf{e_1}$ = (XXX…X 00…0)

$\mathbf{e_2}$ = (000…0 ΔΔ…Δ)

i.e. $\mathbf{e_1} + \mathbf{e_2} = \mathbf{v} + \mathbf{w}$ $(w+v+e_1 = e_2)$

$\Rightarrow w(\mathbf{e_1}) + w(\mathbf{e_2}) = w(\mathbf{v}+\mathbf{w}) = d(\mathbf{v},\mathbf{w}) = d^*$

consider: $r = v+e_1$

$d(r,v) = w(e_1)$

$d(r,w) = w(w+r)$

$= w(w+v+e_1) = w(e_2)$

if $w(e_1) > t$ then $w(e_2) \leq t+1$

i.e. $d(r,v) \geq d(r,w)$ ∴ r 會更正成 w

$\Rightarrow$ incorrect decoding

(ii) ($\leq$ t errors)

Q: pf: $\Rightarrow$

if $d(r,v) \leq t$ i.e. 有 t errors

if z was another codeword

$2t+1 \leq d(v,z) \leq d(v,r) + d(r,z) \leq t + d(r,z)$

$\Rightarrow d(r,z) \geq t + 1$ ∴ r will be correctly decoded into v

Theorem 4 : The code C contains a nonzero codeword c, s.t. $W(c) \le p$ iff a linearly dependent set of p columns of H exists.

p-1

p-1

Proof:

$cH^T=\mathbf{0}$

$$(0,1,1,1,0)\begin{pmatrix}1&0\\0&1\\1&1\\1&0\\0&1\end{pmatrix}=(0,0) \qquad 1\cdot(0,1)+1\cdot(1,1)+1\cdot(1,0)=(0,0)$$

Theorem 4' Let C be an (n,k) linear code with parity-check matrix **H**. For each codeword of Hamming weight l, there exist l columns of **H** such that the vector sum of these l columns is equal to the zero vector. Conversely, if there exist l columns of **H** whose vector sum is the zero vector, there exists a codeword of Hamming weight l in C.

(1) →

(2) ←

$W^* \le p-1$ (→ ←)

Corollary 1 : A code has minimum weight $W^* \ge p$ iff every set of p-1 columns of H is linearly independent

∃ p-1 dep.

Corollary 2 : W^* is equal to the smallest number of columns of H that sum to $\mathbf{0}$.

Pf: By Cor. 1 $W^* \ge p$ & By Th. 4 $W^* \le p$ $\therefore$ $W^* = p$

- (n,k) code corrects t errors ➔ 2t columns of H is linearly independent

$d_1^* \ge 2t+1$

!! Theorem 5 : (singleton Bound)

For (n,k) linear code $d^* \le 1 + n - k$ w^*

- if d^* = 1+n-k ➔ maximum-distance code
- in order to correct t errors, a code must have at least 2t parity symbols, i.e. 2 parity symbols per error to be corrected.

$$2t+1 \le d^* \le 1+n-k$$
$$\Rightarrow \quad n-k \ge 2t$$

Q: 是否會均為1

pf: c = i x G

取 i=(0 0 ... 0 1 0 ... 0)

at least one nonzero

c = [parity check bits i]

至多 n-k 個 “1”

- **Most good codes have a minimum distance well below the bound, but it is sometimes useful.**
- **Most codes , even optimum codes, have considerably more parity symbols than required by the Singleton bound, but some meet it with equality.**

Standard Arrray C = (n,k)

decoding sphere

$2^k \times 2^{n-k}$ (row)

$v_1=0$	v_2	…	v_i	…	v_{2^k}
e_2	$e_2 + v_2$	…	$e_2 + v_i$	…	$e_2 + v_{2^k}$
e_3	$e_3 + v_2$	…	$e_3 + v_i$	…	$e_3 + v_{2^k}$
⋮					⋮
e_l	$e_l + v_2$	…	$e_l + v_i$	…	$e_l + v_{2^k}$
e_{l+1}	$e_{l+1} + v_2$	…	$e_{l+1} + v_i$	…	$e_{l+1} + v_{2^k}$
⋮					⋮
$e_{2^{n-k}}$	$e_{2^{n-k}} + v_2$	…	$e_{2^{n-k}} + v_i$	…	$e_{2^{n-k}} + v_{2^k}$

code words →

one coset of code C

≤ t errors

> t errors

coset leaders

Figure 2. Standard array for an (n,k) linear code

e.g. C=(6,3) $G = \begin{bmatrix} 0&1&1&1&0&0 \\ 1&0&1&0&1&0 \\ 1&1&0&0&0&1 \end{bmatrix}$ $H = \begin{bmatrix} 1&0&0&0&1&1 \\ 0&1&0&1&0&1 \\ 0&0&1&1&1&0 \end{bmatrix}$

single error

Syndrome	Coset leader		v_s	v_i		v_j			
(0 0 0)	000000		011100	101010	110001	110110	101101	011011	000111
(1,0,0)	100000		111100	001010	010001	010110	001101	111011	100111
(0,1,0)	010000		001100	111010	100001	100110	111101	001011	010111
(0,0,1)	001000	e_l	010100 (r)	100010 (x)	111001	111110	100101	010011	001111
(0,1,1)	000100		011000	101110	110101	110010	101001	011111	000011
(1,0,1)	000010		011110	101000	110011	110100	101111	011001	000101
(1,1,0)	000001		011101	101011	110000	110111	101100	011010	000110
(1,1,1)	100100		111000	001110	010101	010010	001001	111111	100011

Figure 3 Standard array for the (6,3) code

correctable error pattern — not correctable error pattern

$= 2^{n-k}$

1. $r = v_j + x = e_l + (v_i + v_j) = e_l + v_s$ ← erroneous decoding

$\uparrow$ noise $= e_l + v_i, v_i \neq 0$

2. $d(r,v_s)=W(r+v_s)=W(e_l+v_s+v_s)=W(e_l)$

$d(r, v_i)=W(r+v_i)=W(e_l+v_s+v_i)=W(e_l+v_j)$

$\because \quad W(e_l) \le W(e_l+v_j)$ ← maximum likelihood decoding

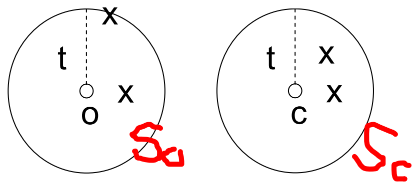
$\therefore \quad d(r, v_s) \le d(r, v_i)$ $\because$

$u-c=v$

$\{ v \mid d(0,v) \le t \} \equiv S_0$

$\{ u \mid d(c,u) \le t \} \approx \{ u \mid d(0,u-c) \le t \} \equiv S_c$

$\therefore \; S_c = S_0 + c = \{ v+c \,(=u) \mid v \in S_0 \}$



Note that : $d(c, v+c)=d(0,v)$

$\therefore$ just record the members of the decoding sphere about all-zero codeword

!! In Fig. 3, just store the 1st column.

Theorem 6 : No two n-tuples in the same row of a standard array are identical. Every n-tuple appears in one and only one row

Pf: (i) $e_l + v_i = e_l + v_j$, $i \neq j \Rightarrow v_i = v_j$ $(\rightarrow\leftarrow)$

(ii) suppose $l < m$ (every n-tuple appears at least one)

$e_l + v_i = e_m + v_j \Rightarrow e_m = e_l + (v_i+v_j) = e_l + v_s$ $(\rightarrow\leftarrow)$

* The decoding is correct iff the error pattern caused by the channel is a coset leader

Theorem 7 : Every (n,k) linear block code is capable of correcting 2^{n-k} error patterns

minimum distance decoding or maximum likelihood decoding

α_i : # of coset leaders of weight i

$$p(E)=1-\sum_{i=0}^{n}\alpha_i p^i(1-p)^{n-i} \text{ : decoding error}$$

eg. $\alpha_0 = 1$ $\alpha_1 = 6$ $\alpha_2 = 1$ $\alpha_3 = \alpha_4 = \alpha_5 = \alpha_6 = 0$

$p = 10^{-2} \Rightarrow p(E) \approx 1.37 \times 10^{-3}$ ← Prob. of decoding error

Theorem 8 : All the 2^k n-tuple of a coset have the same syndrome. The syndromes for different cosets are different.

(i) $(e_l + v_i) H^T = e_l H^T$

(ii) For e_j , e_l $j < l$

if $e_j H^T = e_l H^T \Rightarrow (e_j + e_l)H^T = 0 \Rightarrow e_j + e_l = v_i \Rightarrow e_l = e_j + v_i$ $(\rightarrow\leftarrow)$

Theorem 9: For an (n,k) linear code C with minimum distance d_{min}, all the n-tuple of weight of $t = \lfloor (d_{min} - 1)/2 \rfloor$ or less can be used a coset leaders of a standard array of C. If all the n-tuple of weight t or less are used as coset leaders, there is at least one n-tuple of weight t+1 that cannot be used as a coset leader. (i.e. $d_{min} \geq 2t + 1$)

Reconfirm : an (n,k) linear code with minimum distance d_{min} is capable of correcting all the error patterns of $\lfloor (d_{min} - 1)/2 \rfloor$ or fewer errors, but it is not capable of correcting all the error patterns of weight t+1.

1. $|\{x|\ w(x) \le t\}| \le 2^{n-k}$
2. "<" $\exists$ y s.t. $w(y) > t$ y can be as a coset leader
3. some v , s.t. $w(v) = t+1$ is correctable
   but not all v, $w(v) = t+1$ are correctable

Pf: (1) let $w(x) \le t$
$w(y) \le t$ $\because w(x+y) \le w(x) + w(y) \le 2t < d_{min}$ Q

Suppose x & y exist in the same coset, then x + y is a codeword($\times$)
$\therefore$ x & y can't exist in the same coset $\therefore |\{x|\ w(x) \le t\}| \le 2^{n-k}$

(2) let $w(v) = d_{min}$ and let x,y s.t. (i) $x + y = v$ (ii) x & y don't have nonzero components in common places

$2t+1 \le w(v) = w(x) + w(y) \le 2t+2$

Q: 1. 一定可找出此y
2. $w(y) = t+2$?

$\therefore$ w(x) & w(y) 不能同時皆 $\le t$ 取 $w(y) = t+1$ Then $w(x) = t$ or $t+1$
$\therefore$ If x is used as a coset leader, then y can't be a coset leader

Note that : x & y must be in the same coset
Pf: If x & y were not in the same coset, sayed $x = e_i+v_k$, $y = e_j+v_l$, $i<j$
$\Rightarrow e_i+v_k + e_j+v_l = v \Rightarrow e_i+ e_j+v_s = v \Rightarrow e_j= e_i+v_h$ ($\times$)

Hamming Codes

For GF(2)

(1) if $d^* \ge 3$ then all columns of H are distinct & nonzero (by Cor. 1)
(2) if H has m rows then H can have 2^m-1 columns but no more
$\rightarrow$ $(n,k)=(2^m-1,\ 2^m-1-m)$ ($n-k = m \Rightarrow k=n-m=(2^m-1)-m$)
(3) the vector sum of two columns, say h_i & h_j, must also be a column in H, say , h_l. Thus $h_i + h_j + h_l = 0 \therefore d^* \le 3$ (by Thm. 4) $\therefore d^* = 3$
(4) by Thm. 9 all the (2^m-1)-tuples of weight 1 can be used as coset leaders ($= 2^m-1$ 個) $\because n-k = m$ 共有 2^m cosets $\therefore$ the zero vector & (2^m-1)-tuples of weight 1 form all the coset leaders of the standard array $\rightarrow$ Perfect code

e.g. m=3
(7,4)

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

Q: plot the standard array of (7,4) Hamming Code

- A Hamming code corrects only the error patterns of single error and no others
- The only other nontrivial binary perfect code is the Golay code (23,12).

We may delete any l columns from H. Then, we obtain an (2^m-l-1, 2^m-m-l-1) Shortened Hamming Code with

$n = 2^m - l - 1$

$n - k = m \quad d^* \geq 3$

$\therefore k = 2^m - m - l - 1$

e.g. $H = [\ I_m\ Q\ ]_{m \times (2^m - 1)}$

$H' = [\ I_m\ Q'\ ]_{m \times (2^{m-1})}$

where Q′ is obtained by deleting all the columns of even weight of Q

Q:

(1) no three columns of Q′ add to zero $\therefore d^* \geq 4$

(2) Let h_i (weight = 3) be a column of Q′

$\exists\ h_j, h_l, h_s$, be columns of I_m,

s.t. $h_i + h_j + h_l + h_s = 0$ $\therefore d^* \leq 4$

$d^* = 4$

(3) single error occurs while weight of the syndrome is odd

double errors occurs while weight of the syndrome is even