

中華民國第四十五屆中小學科學展覽會
作品說明書

高中組 數學科

040413

「碼」到成功

高雄市立高雄女子高級中學

作者姓名：

高二 吳怡樺 高二 林筱涵

指導老師：

李奇穎

中華民國第四十五屆中小學科學展覽會
作品說明書

科別：數學科

組別：高中組

作品名稱：「碼」到成功

關鍵字：編碼、最小漢明距

編號：

摘 要

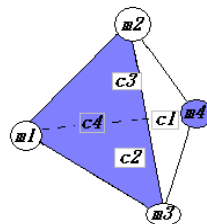
傳輸訊息時，可能因干擾造成誤差。在不複傳情況下，設定檢查碼檢測並校正誤差是個可行方法，而研究出好的檢查碼編碼方式則是我們的目標。

針對 (n,k) 線性區段碼 $X=(m_1 m_2 m_3 \dots m_k c_1 c_2 c_3 \dots c_{n-k})$ ，一組訊息有 n 個比次。前 k 個向量為訊息比次，另外 $n-k$ 個為檢查比次，我們發展出三個較好的編碼方法：

一、四面體編碼：

如圖： $C_q = m_1 \oplus m_2 \oplus m_3 \oplus m_4 - m_q$

$$q = 1, 2, 3, 4$$



此編碼的最小漢明距($d_{\min}$)=4，碼速= $\frac{4}{8}$ 。可偵測二個誤差且校正一個誤差。此編碼法可

推廣至 (n,k) $n=2k$ ($k \in \mathbb{N}$)形式，且碼速和 $d_{\min}$ 不變。

二、六面體編碼

$$C_q = m_{s_1} \oplus m_{s_2} \oplus m_{s_3} \oplus m_j, \quad q = 1, 2, 3, 4, 5, 6, \quad s_1, s_2, s_3 \in \{1, 2, 3, \dots, 8\} \quad s_1 \neq s_2 \neq s_3$$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \pmod{6}, \quad q \equiv j \pmod{2} \quad j = 7, 8$$

此編碼 $d_{\min}=4$ ，可偵測二個誤差且校正一個誤差，碼速= $\frac{8}{14}$ 。此編碼法亦可推廣至

$(14R, 8R)$ $R \in \mathbb{N}$ 線性區段碼，而 $d_{\min}$ 不變。

三、十二面體編碼

$$C_q = m_{s_1} \oplus m_{s_2} \oplus m_{s_3} \oplus m_j \oplus m_k, \quad q = 1, 2, 3, \dots, 12, \quad s_1, s_2, s_3 \in \{1, 2, 3, \dots, 12\}$$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \pmod{12}, \quad q \equiv j \pmod{4}, \quad j = 13 \sim 16$$

$$q \equiv k \pmod{2} \begin{cases} q = 1 \sim 6 \text{ 時} \Rightarrow k = 17 \text{ or } 18 \\ q = 7 \sim 12 \text{ 時} \Rightarrow k = 19 \text{ or } 20 \end{cases}$$

此編碼 $d_{\min}=4$ ，可偵測二個誤差且校正一個誤差，碼速= $\frac{20}{32}$ 。此編碼法亦可推廣至

$(32R, 20R)$ 線性區段碼，而 $d_{\min}$ 不變。

目 錄

壹、	研究動機	2
貳、	研究目的	2
參、	研究設備與器材	2
肆、	研究過程	2
一、	蜂窩形編碼	2
二、	四面體編碼	5
三、	四面體編碼之延伸	7
四、	六面體編碼	10
五、	六面體編碼之延伸	12
六、	十二面體編碼	14
七、	十二面體編碼之延伸	17
伍、	研究結果	19
陸、	討論	20
柒、	結論	20
捌、	參考資料及其他	20
一、	文獻整理	20
二、	參考書籍	26
三、	附錄	26

壹、 研究動機

一年級上地球科學時，課本寫到：織女星離我們 26 光年。即在地球上接收到的光是 26 年前的光；太空船傳回的資訊也像我們接收到織女星上的光一樣，是很久以前的資料。如果傳送過程中受到干擾，那接受到的資訊也可能是錯誤的，但是這些資料並不能複傳，所以必須有一種良好的傳輸方法，使我們能偵測並校正誤差。所以我們開始研究在無複傳的狀況下，可校正誤差的編碼法。

貳、 研究目的

在無法複傳的情況下，傳輸的訊息只能依靠有效的檢查法做校正的工作。而我們的研究目的是希望架構一種編碼法，使其能夠偵測並校正所傳輸的訊息。

參、 研究設備與器材

電腦、紙、筆

肆、 研究過程

在以下的編碼法中，我們利用到 P22 的二元(binary)加法運算：

$$0 \oplus 0 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 1 \oplus 1 = 0$$

由上面四個式子可知： $a \oplus b = a - b$

一、蜂窩形編碼

(一) 定義:

1. 編碼方法

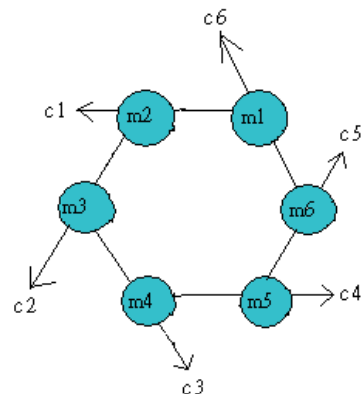
(1). 訊息比次 m_x

(2). 檢查碼 c_y

$$c_1 = m_1 \oplus m_2$$

$$c_2 = m_2 \oplus m_3$$

$$c_3 = m_3 \oplus m_4$$



$$c_4 = m_4 \oplus m_5$$

$$c_5 = m_5 \oplus m_6$$

$$c_6 = m_6 \oplus m_1$$

2. 生成矩陣:

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

(二) 分析

1. 單一誤差

(1). m_x 發生錯誤: 可偵測並校正

(2). c_y 發生錯誤: 可偵測並校正

2. 雙重誤差

(1). 若錯二個 m 則

i. 可偵錯但不可校正

如: $m_1 m_2$ 錯, $c_2 c_6$ 會反應, c_1 不會反應, 會誤判 $c_2 c_6$ 錯, 故只可偵測不可校正。 $(m_x m_{x+1}$ 錯, 則誤判 $c_{x-1} c_{x+1}$)

ii. 可校正

如 $m_1 m_3$ 錯, $c_1 c_2 c_3 c_6$ 會反應, 可推測 $m_1 m_3$ 錯。

(2). 若錯二個 c

i. 可偵測, 不可校正

a. 錯 $c_x c_{x+1}$ 誤判 m_{x+1}

如: $c_1 c_2$ 錯, 會誤判 m_2 , 故只可偵錯

b. 錯 $c_x c_{x+2}$ 誤判 $m_{x+1} m_{x+2}$

如 $c_1 c_3$ 錯, 會誤判 $m_2 m_3$, 故只可偵錯

c. 錯 $c_x c_{x+4}$ 誤判 $m_x m_{x+5}$

如 $c_1 c_5$ 錯, 會誤判 $m_1 m_6$, 故只可偵錯

ii. 可校正: 錯 $c_x c_{x+3}$ 可推測 $c_x c_{x+3}$ 錯

如: $c_1 c_4$ 錯, 可推測 $c_1 c_4$ 錯

(3). 若錯一個 c 一個 m 則

i. 可偵測, 不可校正

如: 錯 $c_1 m_1$ 則只有 c_6 反應, 可能誤判 c_6 錯。

ii. 可校正

如:錯 c_1m_4 則 $c_1c_3c_4$ 有反應，可推測 c_1m_4 錯。

3. 歸納

(1).單一誤差皆可校正

(2).雙重誤差可校正有 24 個， 只可偵測有 42 個

(三) 蜂窩型編碼最小漢明距的計算過程

假設有兩組訊息分別為： $m_{11}m_{12}m_{13}m_{14}m_{15}m_{16}c_{11}c_{12}c_{13}c_{14}c_{15}c_{16}$

$$m_{21}m_{22}m_{23}m_{24}m_{25}m_{26}c_{21}c_{22}c_{23}c_{24}c_{25}c_{26}$$

$$A = \{i | \alpha_i = 1 \text{ 且 } i = 1, 2, 3, 4, 5, 6\} \quad B = \{j | \alpha_j = 0 \text{ 且 } j = 1, 2, 3, 4, 5, 6\} \quad i \neq j$$

定義 α, β 如右： $m_{1p} \oplus m_{2p} = \alpha_p \quad c_{1p} \oplus c_{2p} = \beta_p \quad p = 1, 2, 3, 4, 5, 6$

1. 一個不同

$$n(A) = 1 \Rightarrow n(B) = 5$$

$$\beta_i = C_{1i} + C_{2i} = m_{1i} + m_{1(i+1)} + m_{2i} + m_{2(i+1)} = \alpha_i + \alpha_{i+1} = 1$$

$$\beta_j = C_{1j} + C_{2j} = m_{1j} + m_{1(j+1)} + m_{2j} + m_{2(j+1)} = \alpha_j + \alpha_{j+1} = \begin{cases} 0 \Rightarrow j+1 \not\equiv 1 \pmod{6} \\ 1 \Rightarrow j+1 \equiv 1 \pmod{6} \end{cases}$$

$$\text{漢明距} = 1 + 1 + 1 = 3$$

2. 二個不同

$$n(A) = 2 \Rightarrow n(B) = 4$$

(1).連續

$$\alpha_i = \alpha_{i+1} = 1 \text{ 且 } j \neq i, i+1$$

$$\beta_i = C_{1i} + C_{2i} = m_{1i} + m_{1(i+1)} + m_{2i} + m_{2(i+1)} = \alpha_i + \alpha_{i+1} = 0$$

$$\beta_{i+1} = C_{1(i+1)} + C_{2(i+1)} = m_{1(i+1)} + m_{1(i+2)} + m_{2(i+1)} + m_{2(i+2)} = \alpha_{i+1} + \alpha_{i+2} = 1$$

$$\beta_j = C_{1j} + C_{2j} = m_{1j} + m_{1(j+1)} + m_{2j} + m_{2(j+1)} = \alpha_j + \alpha_{j+1} = \begin{cases} 0 \Rightarrow j+1 \not\equiv 1 \pmod{6} \\ 1 \Rightarrow j+1 \equiv 1 \pmod{6} \end{cases}$$

$$\text{漢明距} = 2 + 1 + 1 = 4$$

(2).不連續

$$\alpha_i = \alpha_{i+k} = 1 \text{ 且 } k \neq 1$$

$$\beta_i = C_{1i} + C_{2i} = m_{1i} + m_{1(i+1)} + m_{2i} + m_{2(i+1)} = \alpha_i + \alpha_{i+1} = 1$$

$$\beta_{i+k} = C_{1(i+k)} + C_{2(i+k)} = m_{1(i+k)} + m_{1(i+k+1)} + m_{2(i+k)} + m_{2(i+k+1)} = \alpha_{(i+k)} + \alpha_{(i+k+1)} = 1$$

$$\text{漢明距}=2+1+1+1+1=6$$

(四) 結果

由之前漢明距的求法可知：蜂窩編碼之最小漢明距 $3 < \text{生成矩陣的漢明距 } 4$ 。又由 P22 的文獻知：最小漢明距=3 可做到每個字元內校正達一個誤差且偵測一個誤差，但蜂窩編碼在某些狀況下會產生誤判，也許可由改變編碼法而得到更進一步的發展。

於是我們嘗試思考柏拉圖多面體(正四面體、正六面體、正八面體、正十二面體及正二十面體)。我們以頂點當作資料碼、面當作檢查碼。因為正八面體及正二十面體的頂點個數少於面的個數，碼速分別為 $\frac{6}{14}$ 、 $\frac{12}{32}$ ，小於 0.5，故不予討論。

二、四面體編碼

(一) 定義

1.編碼方式：此種編碼方式是一對三的

也就是說：如果有一個訊息碼錯誤，則有三個檢查碼會反應出來，而三個檢查碼的交點即為錯誤所在。

(1).訊息比次 m_x ：如右上圖。

(2).檢查碼 c_x ： m_x 在另外三個點所圍成的平面上的投影點，如圖 2。

$$C_1 = m_2 \oplus m_3 \oplus m_4$$

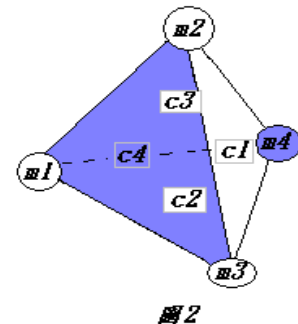
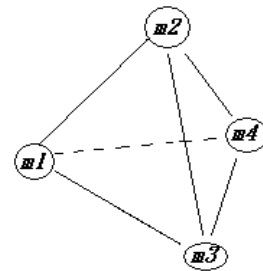
$$C_2 = m_1 \oplus m_3 \oplus m_4$$

$$C_3 = m_1 \oplus m_2 \oplus m_4$$

$$C_4 = m_1 \oplus m_2 \oplus m_3$$

$$\text{即：} C_q = m_1 \oplus m_2 \oplus m_3 \oplus m_4 - m_q \quad q = 1, 2, 3, 4$$

2.生成矩陣



$$\text{四面體編碼的生成矩陣如右：} G = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array} \right] \\ = [M \quad | \quad C]$$

M 為 4×4 單位矩陣, C 為單位矩陣所產生之檢查矩陣。任一系列的 M 矩陣中其順序分別為 $m_1 m_2 m_3 m_4$; 任一系列的 C 矩陣中其順序分別為 $c_1 c_2 c_3 c_4$

假設有兩組訊息分別為： $m_{11} m_{12} m_{13} m_{14} c_{11} c_{12} c_{13} c_{14}$

$$m_{21} m_{22} m_{23} m_{24} c_{21} c_{22} c_{23} c_{24}$$

並 α, β 定義如右： $m_{1p} \oplus m_{2p} = \alpha_p \quad c_{1p} \oplus c_{2p} = \beta_p \quad p=1,2,3,4$

$$A = \{i | \alpha_i = 1 \wedge i = 1, 2, 3, 4\}, B = \{j | \alpha_j = 0 \wedge j = 1, 2, 3, 4\}, i \neq j$$

由生成矩陣中明顯看出 $n(A) = 2 \Rightarrow n(B) = 2$

$$\therefore \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 = 0$$

$$\begin{aligned} \beta_i &= c_{1i} \oplus c_{2i} & \beta_j &= c_{1j} \oplus c_{2j} \\ &= m_{11} \oplus m_{12} \oplus m_{13} \oplus m_{14} - m_{1i} & &= m_{11} \oplus m_{12} \oplus m_{13} \oplus m_{14} - m_{1j} \\ &\quad \oplus m_{21} \oplus m_{22} \oplus m_{23} \oplus m_{24} - m_{2i} & &\oplus m_{21} \oplus m_{22} \oplus m_{23} \oplus m_{24} - m_{2j} \\ &= \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 - \alpha_i & &= \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 - \alpha_j \\ &= 0 - 1 & &= 0 - 0 \\ &= 1 & &= 0 \end{aligned}$$

$\therefore$ 生成矩陣的最小漢明距($d_{\min}$) = 4

(二) 編碼後資料之最小漢明距

假設有兩組訊息分別為： $m_{11} m_{12} m_{13} m_{14} c_{11} c_{12} c_{13} c_{14}$

$$m_{21} m_{22} m_{23} m_{24} c_{21} c_{22} c_{23} c_{24}$$

註： $C_q = m_1 \oplus m_2 \oplus m_3 \oplus m_4 - m_q \quad q=1,2,3,4$

並 α, β 定義如右： $m_{1p} \oplus m_{2p} = \alpha_p \quad c_{1p} \oplus c_{2p} = \beta_p \quad p=1,2,3,4$

$$A = \{i | \alpha_i = 1 \wedge i = 1, 2, 3, 4\}, B = \{j | \alpha_j = 0 \wedge j = 1, 2, 3, 4\}, i \neq j$$

$$1. n(A) = 1 \Rightarrow n(B) = 3$$

$$\because \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 = 1$$

$$\Rightarrow 4 \text{ 個 } \beta \text{ 中有 } 3 \text{ 個 } 1 \Rightarrow d = 1 + 3 = 4$$

$$2. n(A) = 2 \Rightarrow n(B) = 2$$

$$\because \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 = 0$$

$$\Rightarrow 4 \text{ 個 } \beta \text{ 中有 } 2 \text{ 個 } 1 \Rightarrow d = 2 + 2 = 4$$

$$3. n(A) = 3 \Rightarrow n(B) = 1$$

$$\because \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 = 1$$

$$\Rightarrow 4 \text{ 個 } \beta \text{ 中有 } 1 \text{ 個 } 1 \Rightarrow d = 3 + 1 = 4$$

$$4. n(A) = 4 \Rightarrow d \geq 4$$

由以上討論可知四面體編碼之 $d_{\min} = 4$

(三) 結果

由四面體編碼的生成矩陣和編碼後資料之最小漢明距的討論得：四面體編碼的 $d_{\min}$ 和其生成矩陣的 $d_{\min}$ 同為 4。由 P22 之文獻：(2)碼向量及漢明距應用可知：
 $s = 2, t = 1 \Rightarrow$ 每個字元內可偵測 2 個誤差且校正達 1 個誤差

三、四面體編碼之延伸

(一) 定義

一個 $(n, k), n=2k$ 的編碼中，每個 c 控制 $k-i$ 個 m ，令 $k-i=l$

即：每組訊息中之編碼順序為 $m_1 m_2 \cdots m_k c_1 c_2 \cdots c_k$

m 為訊息比次； c 為檢查比次

$$c \text{ 之定義爲： } c_q = m_1 \oplus m_2 \oplus \dots \oplus m_k - m_{s_1} - m_{s_2} - \dots - m_{s_i} \quad q=1 \sim k$$

$$q \equiv s_1 + i \equiv s_2 + (i-1) \equiv \dots \equiv s_i + 1 \pmod{k} \quad s_1, s_2, \dots, s_i \in \{1, 2, 3, \dots, k\}$$

(二) 最小漢明距的計算過程

假設有兩組訊息分別爲： $m_{11} m_{12} \dots m_{1k} c_{11} c_{12} \dots c_{1k}$

$$m_{21} m_{22} \dots m_{2k} c_{21} c_{22} \dots c_{2k}$$

並 α, β 定義如右： $m_{1p} \oplus m_{2p} = \alpha_p$; $c_{1q} \oplus c_{2q} = \beta_q$ $p=1, 2, \dots, k$; $q=1, 2, \dots, k$

$$A = \{i | \alpha_i = 1 \wedge i = 1, 2, \dots, k\}, B = \{j | \alpha_j = 0 \wedge j = 1, 2, \dots, k\}, i \neq j$$

$$\begin{aligned} \therefore \beta_q &= c_{1q} \oplus c_{2q} \\ &= m_{11} \oplus m_{12} \oplus \dots \oplus m_{1k} - m_{1s_1} - m_{1s_2} - \dots - m_{1s_i} \\ &\quad \oplus m_{21} \oplus m_{22} \oplus \dots \oplus m_{2k} - m_{2s_1} - m_{2s_2} - \dots - m_{2s_i} \\ &= \alpha_1 \oplus \alpha_2 \dots \oplus \alpha_k - \alpha_{s_1} - \alpha_{s_2} - \dots - \alpha_{s_i} \end{aligned}$$

$$q \equiv s_1 + i \equiv s_2 + (i-1) \equiv \dots \equiv s_i + 1 \pmod{k} \quad s_1, s_2, \dots, s_i \in \{1, 2, 3, \dots, k\}$$

$$k - i = l$$

$$1. n(A) = 1 \Rightarrow n(B) = k - 1$$

$$\therefore \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \alpha_1 \oplus \alpha_2 \oplus \dots \oplus \alpha_k = 1$$

$$\Rightarrow \beta_q = 1 \text{ 有 } k-i \text{ 個 } \Rightarrow d = 1 + k - i = 1 + l$$

$$2. n(A) = 2 \Rightarrow n(B) = k - 2$$

$$\text{令 } \alpha_i = 1, \alpha_{i+t} = 1 \quad t \in \mathbb{N}$$

$$(1). t \leq l$$

$$\text{當 } q + l - 1 = i \dots (i + t - 1) \text{ 時, } \beta_q = 1 \quad \text{共有 } (i + t - 1) - i + 1 = t \text{ 個 } 1$$

$$\text{當 } q = (i + 1) \dots (i + t) \text{ 時, } \beta_q = 1 \quad \text{共有 } (i + t) - (i + 1) + 1 = t \text{ 個 } 1$$

所以 $\beta_q = 1$ 有 $2t$ 個 $1 \Rightarrow d = 2 + 2t$

(2). $t > l$

當 $i = q \dots (q+l-1)$ 時, $\beta_q = 1$ 共有 $(q+l-1) - q + 1 = l$ 個 1

當 $i+t = q \dots (q+l-1)$ 時, $\beta_q = 1$ 共有 $(q+l-1) - q + 1 = l$ 個 1

所以 β_q 有 $2l$ 個 $1 \Rightarrow d = 2 + 2l$

3. $n(A) \geq 3 \Rightarrow n(B) \leq k - 3$

令 $\alpha_i = 1, \alpha_j = 1, \alpha_k = 1$

由 $n(A) = 2$ 的結果可知: $\beta_q = 1$ 的個數皆為正偶數($2t$ 或 $2l$ 個)

$\therefore$ 先考慮 α_i, α_j 則

(1). $\beta_q = 1$ 的個數有 2 個

再考慮 α_k , 因為有三個 β_q 中含 α_k

所以若上面兩個 $\beta_q = 1$ 均被修正為 0, 則必另有一 β_q 由 0 變為 1

若上面兩個 $\beta_q = 1$ 不全被修正為 0, 則至少有一個 $\beta_q = 1$

(2). $\beta_q = 1$ 的個數為大於等於 4 的正偶數

再考慮 α_k , 因為有三個 β_q 中含 α_k

上面的 $\beta_q = 1$ 中最多只有 3 個被修正為 0, 所以 $\beta_q = 1$ 的個數至少為 1

由上述(1)(2)可得: $d \geq 4$

綜合上面三點, 此種編碼之最小漢明距 =
$$\begin{cases} 1+l & l < 3 \\ 4 & l \geq 3 \end{cases}$$

(三) 結果

若要求四面體編碼之延伸的 $d_{\min} = 4$, 則 $l \geq 3$

再由 P22 之文獻可知: $s=2, t=1 \Rightarrow$ 每個字元內可偵測 2 個誤差且校正達 1 個誤差。

四、六面體編碼

(一) 定義

一個 $(n,k)=(14,8)$ 的編碼中，每個 c 控制 4 個 m ，一個 m 被 3 個 c 檢查

即：每組訊息中之編碼順序為 $m_1 m_2 \cdots m_8 c_1 c_2 \cdots c_6$

m 為訊息比次； c 為檢查比次

c 之定義為：

$$c_q = m_{s_1} \oplus m_{s_2} \oplus m_{s_3} \oplus m_j \quad q=1,2,3,\cdots,6 \quad s_1, s_2, s_3 \in \{1,2,3,\cdots,6\} \quad s_1 \neq s_2 \neq s_3$$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \pmod{6}, \quad q \equiv j \pmod{2} \quad j=7,8$$

詳見附錄之表(一)

(二) 最小漢明距的計算

假設有兩組訊息分別為： $m_{11} m_{12} \cdots m_{18} c_{11} c_{12} \cdots c_{16}$

$$m_{21} m_{22} \cdots m_{28} c_{21} c_{22} \cdots c_{26}$$

並 α, β 定義如右： $m_{1p} \oplus m_{2p} = \alpha_p$ ； $c_{1q} \oplus c_{2q} = \beta_q$ $p=1,2,\dots,8$ ； $q=1,2,\dots,6$

$$A = \{i | \alpha_i = 1 \wedge i = 1, 2, \dots, 8\}, B = \{j | \alpha_j = 0 \wedge j = 1, 2, \dots, 8\}, i \neq j$$

$$\therefore \beta_q = \alpha_{s_1} \oplus \alpha_{s_2} \oplus \alpha_{s_3} \oplus \alpha_j \quad s_1, s_2, s_3 \in \{1, 2, 3, \dots, 6\} \quad s_1 \neq s_2 \neq s_3$$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \pmod{6} \quad q \equiv j \pmod{2} \quad j=7,8$$

$$1. n(A) = 1$$

$\because$ 1 個 m 被三個 c 檢查

$$\Rightarrow \beta_q (q=1,2,3,4,5,6) \text{ 中有 3 個 } 1 \Rightarrow d = 1+3 = 4$$

$$2. n(A) = 2$$

$$\alpha_i = 1, \alpha_{i+t} = 1, t \in \mathbb{N}$$

$$\text{令 } v = i + t \quad C = \{1, 2, 3, 4, 5, 6\} \quad D = \{7, 8\}$$

(1). $i, v \in C$

i. $t \leq 3$

當 $q+2=i \cdots (i+t-1)$ 時, $\beta_q = 1$ 共有 $(i+t-1)-i+1=t$ 個 1

當 $q=(i+1) \cdots (i+t)$ 時, $\beta_q = 1$ 共有 $(i+t)-(i+1)+1=t$ 個 1

所以 β_q 只有 $2t$ 個 1 $\Rightarrow d = 2 + 2t \geq 4$

(2). $t > 3$

當 $i = q \cdots (q+3-1)$ 時, $\beta_q = 1$ 共有 $(q+3-1)-q+1=3$ 個 1

當 $i+t = q \cdots (q+3-1)$ 時, $\beta_q = 1$ 共有 $(q+3-1)-q+1=3$ 個 1

所以 β_q 有 6 個 1 $\Rightarrow d = 2 + 6 = 8$

(3). $i, j \in D$

$\because$ 檢查碼所檢查的訊息比次互斥 $\therefore d = 2 + 6 = 8$

(4). $i \in C, j \in D$

i. 若 i 為奇數且 j 為奇數

有兩個 β 只含 α_i, α_j 兩者之一, 所以這兩個 $\beta = 1 \Rightarrow d = 2 + 2 = 4$

ii. 若 i 為奇數且 j 為偶數

有四個 β 只含 α_i, α_j 兩者之一, 所以這四個 $\beta = 1 \Rightarrow d = 2 + 4 = 6$

iii. 若 i 為偶數且 j 為偶數

有兩個 β 只含 α_i, α_j 兩者之一, 所以這兩個 $\beta = 1 \Rightarrow d = 2 + 2 = 4$

iv. 若 i 為偶數且 j 為奇數

有四個 β 只含 α_i, α_j 兩者之一, 所以這四個 $\beta = 1 \Rightarrow d = 2 + 4 = 6$

$\therefore n(A) = 2$ 時的 $d_{\min} = 4 \Rightarrow$ 至少存在兩個 $\beta_q = 1$

(3) $n(A) = 3$

令 $\alpha_i = 1, \alpha_j = 1, \alpha_k = 1$

由 $n(A) = 2$ 的結果可知: $\beta_q = 1$ 的個數可能為 2 個、4 個或 6 個

先考慮 α_i, α_j 則

(1). $\beta_q = 1$ 的個數為 2 個

再考慮 α_k , 因為有三個 β_q 中含 α_k

所以若上面兩個 $\beta_q = 1$ 均被修正為 0, 則必有一 β_q 由 0 變為 1

若上面兩個 $\beta_q = 1$ 不全被修正為 0, 則至少有一個 $\beta_q = 1$

(2). $\beta_q = 1$ 的個數為 4 個

再考慮 α_k , 因為有三個 β_q 中含 α_k

上面四個 $\beta_q = 1$ 最多只有 3 個被修正為 0, 所以 $\beta_q = 1$ 的個數至少為 1, $\therefore d \geq 4$

由上述之(1)(2) $\Rightarrow d \geq 3+1=4$

綜合以上三點, 可得 $d_{\min} = 4$

五、六面體編碼之延伸

(一) 定義

一個 $(n, k) = (14R, 8R), R \in \mathbb{N}$ 的編碼中, 每個 c 控制 4 個 m , 每一個 m 被 3 個 c 檢查

即: 每組訊息中之編碼順序為 $m_1 m_2 \cdots m_{8R} c_1 c_2 \cdots c_{6R}$

m 為訊息比次; c 為檢查比次

c 之定義為:

$$c_q = m_{s_1} \oplus m_{s_2} \oplus m_{s_3} \oplus m_j \quad q = 1, 2, 3, \dots, 6R \quad s_1, s_2, s_3 \in \{1, 2, 3, 4, 5, 6\}$$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \pmod{6R} \quad q \equiv j \pmod{2R}, \quad j = 6R+1, 6R+2, \dots, 8R$$

(二) 最小漢明距的計算過程

假設有兩組訊息分別為: $m_{11} m_{12} \cdots m_{1(8R)} c_{11} c_{12} \cdots c_{1(6R)}$

$$m_{21}m_{22} \cdots m_{2(8R)}c_{21}c_{22} \cdots c_{2(6R)}$$

並 α, β 定義如右： $m_{1p} \oplus m_{2p} = \alpha_p$ ； $c_{1q} \oplus c_{2q} = \beta_q$ $p=1,2,\dots,8R$ ； $q=1,2,\dots,6R$

$$A = \{i | \alpha_i = 1 \wedge i = 1, 2, \dots, 8R\}, B = \{j | \alpha_j = 0 \wedge j = 1, 2, \dots, 8R\}, i \neq j$$

$$1. n(A) = 1$$

$\therefore$ 每個 m 被三個 c 控制 $\therefore$ 有三個 $\beta = 1$

$$\Rightarrow d = 1 + 3 = 4$$

$$2. n(A) = 2$$

$$\alpha_i = 1, \alpha_{i+t} = 1, t \in \mathbb{N}$$

$$\text{令 } v = i + t \quad C = \{1, 2, 3, \dots, 6R\} \quad D = \{6R+1, 6R+2, \dots, 8R\}$$

$$(1). i, v \in C$$

$$i. t \leq 3$$

當 $q+2 = i \cdots (i+t-1)$ 時, $\beta_q = 1$ 共有 $(i+t-1) - i + 1 = t$ 個 1

當 $q = (i+1) \cdots (i+t)$ 時, $\beta_q = 1$ 共有 $(i+t) - (i+1) + 1 = t$ 個 1

所以 β_q 有 $2t$ 個 1 $\Rightarrow d = 2 + 2t \geq 4$

$$ii. t > 3$$

當 $i = q, (q+1), (q+2)$ 時, $\beta_q = 1$

當 $i+t = q, (q+1), (q+2)$ 時, $\beta_q = 1$

$$\Rightarrow d = 2 + 6 = 8$$

$$(2). i, v \in D$$

$\therefore$ 檢查碼所檢查的訊息比次互斥 $\therefore d = 2 + 6 = 8$

$$(3). i \in C, v \in D$$

$\therefore \alpha_i$ 對應連續三個 β, α_j 對應到的 β 間隔 $2R$

$$\therefore \begin{cases} R=1 \text{ 時} & d \begin{cases} 2+2=4 \\ 2+4=6 \end{cases} \text{ or } \\ R \geq 2 \text{ 時} & d \begin{cases} 2+4=6 \\ 2+6=8 \end{cases} \text{ or } \end{cases}$$

$\Rightarrow n(A) = 2$ 時的 $d = 4 \Rightarrow$ 至少存在兩個 $\beta_q = 1$

$$3. n(A) = 3$$

$$\text{令 } \alpha_i = 1, \alpha_j = 1, \alpha_k = 1$$

由 $n(A) = 2$ 的結果可知： $\beta_q = 1$ 的個數可能為 2 個、4 個或 6 個

先考慮 α_i, α_j 則

(1). $\beta_q = 1$ 的個數為 2 個

再考慮 α_k , 因為有三個 β_q 中含 α_k

所以若上面兩個 $\beta_q = 1$ 均被修正為 0, 則必有一 β_q 由 0 變為 1

若上面兩個 $\beta_q = 1$ 不全被修正為 0, 則至少有一個 $\beta_q = 1$

(2). $\beta_q = 1$ 的個數為 4 個

再考慮 α_k , 因為有三個 β_q 中含 α_k

上面四個 $\beta_q = 1$ 最多只有 3 個被修正為 0, 所以 $\beta_q = 1$ 的個數至少為 1, $\therefore d \geq 4$

由上述之(1)(2) $\Rightarrow d \geq 3 + 1 = 4$

綜合以上三點, 可得 $d_{\min} = 4$

六、十二面體編碼

(一)定義:

一個 $(n, k) = (32, 20)$ 的編碼中, 每個 c 控制 5 個 m , 每一個 m 被 3 個 c 檢查

即: 每組訊息之編碼順序為 $m_1 m_2 \cdots m_{20} c_1 c_2 \cdots c_{12}$, m 為訊息比次; c 為檢查比次

c 之定義為: $c_q = m_{s_1} \oplus m_{s_2} \oplus m_{s_3} \oplus m_j \oplus m_k \quad q = 1, 2, 3, \cdots, 12 \quad s_1, s_2, s_3 \in \{1, 2, 3, \cdots, 12\}$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \pmod{12} \quad q \equiv j \pmod{4}, j = 13 \sim 16$$

$$q \equiv k \pmod{2} \begin{cases} q = 1 \sim 6 \text{ 時} \Rightarrow k = 17 \text{ or } 18 \\ q = 7 \sim 12 \text{ 時} \Rightarrow k = 19 \text{ or } 20 \end{cases}$$

詳見附錄之表(二)

(二)最小漢明距的計算過程

假設有兩組訊息分別為：

$$m_{11}m_{12} \cdots m_{120}c_{11}c_{12} \cdots c_{112}$$

$$m_{21}m_{22} \cdots m_{220}c_{21}c_{22} \cdots c_{212}$$

並 α, β 定義如右： $m_{1p} \oplus m_{2p} = \alpha_p$; $c_{1q} \oplus c_{2q} = \beta_q$ $p=1, 2, \dots, 20$ $q=1, 2, \dots, 12$

$$A = \{i | \alpha_i = 1 \wedge i = 1, 2, \dots, 20\}, B = \{j | \alpha_j = 0 \wedge j = 1, 2, \dots, 20\}, i \neq j$$

$$1. n(A) = 1 \Rightarrow n(B) = 20 - 1 = 19 \Rightarrow \beta \text{ 有 } 3 \text{ 個 } 1 \Rightarrow d = 1 + 3 = 4$$

$$2. n(A) = 2 \Rightarrow n(B) = 20 - 2 = 18$$

$$\alpha_i, \alpha_{i+t} = 1$$

$$(1). i, i+t \in 1 \sim 12$$

$$i. t \leq 3$$

當 $q+3-1=i \cdots (i+t-1)$ 時, $\beta_q = 1$ 共有 $(i+t-1)-i+1=t$ 個 1

當 $q=(i+1) \cdots (i+t)$ 時, $\beta_q = 1$ 共有 $(i+t)-(i+1)+1=t$ 個 1

所以 β_q 有 $2t$ 個 1 $\Rightarrow d = 2 + 2t \geq 4$

$$ii. t > 3$$

當 $i=q \cdots (q+3-1)$ 時, $\beta_q = 1$ 共有 $(q+3-1)-q+1=3$ 個 1

當 $i+t=q \cdots (q+3-1)$ 時, $\beta_q = 1$ 共有 $(q+3-1)-q+1=3$ 個 1

所以 β_q 有 6 個 1 $\Rightarrow d = 2 + 6 = 8$

$$(2). i, i+t \in 13 \sim 16$$

$\because$ 每個 m 被 3 個 C 控制且每個 m 對應到的 c 均不重複

$$\therefore d = 2 + 6 = 8$$

$$(3). i, i+t \in 17 \sim 20$$

$\because$ 每個 m 被 3 個 C 控制且每個 m 對應到的 c 均不重複

$$\therefore d = 2 + 6 = 8$$

$$(4). i \in 1 \sim 12, i+t \in 13 \sim 16$$

$\because \alpha_i$ 對應連續 3 個 c, α_j 對應到的 c 間隔 4

$$\therefore d = \begin{cases} 2+4=6 \\ or \\ 2+6=8 \end{cases}$$

$$(5). i \in 1 \sim 12, i+t \in 17 \sim 20$$

$\therefore \alpha_i$ 對應連續 3 個 c , α_j 對應到的 c 間隔 2

$$\therefore d = \begin{cases} 2+2=4 \\ or \\ 2+4=6 \end{cases}$$

$$(6). i \in 13 \sim 16, i+t \in 17 \sim 20$$

$$\therefore i \equiv q \pmod{4} \quad (i+t) \equiv q \pmod{2}$$

$\therefore \beta$ 必不全相同 $\Rightarrow$ 存在一個 β 只含 α_i , 不含 α_{i+t} , 且存在一個 β 只含 α_{i+t} , 不含 α_i

故 $d \geq 2+2=4$

$$3. \quad n(A) \geq 3 \Rightarrow n(B) \leq k-3$$

令 $\alpha_i = 1$, $\alpha_j = 1$, $\alpha_k = 1$

由 $n(A) = 2$ 的結果可知: $\beta_q = 1$ 的個數有 2 個、4 個和 6 個

先考慮 α_i, α_j 則

$$(1). \beta_q = 1 \text{ 的個數為 } 2 \text{ 個}$$

再考慮 α_k , 因為有三個 β_q 中含 α_k

所以若上面兩個 $\beta_q = 1$ 均被修正為 0, 則必有一 β_q 由 0 變為 1

若上面兩個 $\beta_q = 1$ 不全被修正為 0, 則至少有一個 $\beta_q = 1$

$$(2). \beta_q = 1 \text{ 的個數為 } 4 \text{ 個}$$

再考慮 α_k , 因為有三個 β_q 中含 α_k

所以上面四個 $\beta_q = 1$ 最多只有 3 個被修正為 0, 所以 $\beta_q = 1$ 的個數至少為 1

由上述(1)(2)可得 $d \geq 4$
 綜合以上三點，最小漢明距為 4

七、十二面體編碼之延伸

(一)定義：

一個 $(n,k)=(32R,20R)$ 的編碼中，每個 c 控制 5 個 m ，每一個 m 被 3 個 c 檢查
 即：每組訊息之編碼順序為 $m_1 m_2 \cdots m_{20R} c_1 c_2 \cdots c_{12R}$

m 為訊息比次； c 為檢查比次

c 之定義為：

$$c_q = m_{s_1} + m_{s_2} + m_{s_3} + m_j + m_k \quad q = 1, 2, 3, \dots, 12R \quad s_1, s_2, s_3 \in \{1, 2, 3, \dots, 12R\}$$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \pmod{12R} \quad q \equiv j \pmod{4R}, j = (12R+1) \sim 16R$$

$$q \equiv k \pmod{2R} \begin{cases} q = 1 \sim 6R \text{ 時} \Rightarrow k = (16R+1) \sim (16R+2R) \\ q = (6R+1) \sim 12R \text{ 時} \Rightarrow k = (16R+2R+1) \sim (16R+4R) \end{cases}$$

(二) 最小漢明距的計算過程：

$$1. n(A) = 1 \Rightarrow n(B) = 20R - 1$$

$$\Rightarrow \beta \text{ 有 } 3 \text{ 個 } 1 \Rightarrow d = 1 + 3 = 4$$

$$2. n(A) = 2 \Rightarrow n(B) = 20R - 2$$

$$\alpha_i, \alpha_{i+t} = 1$$

$$(1). i, i+t \in 1 \sim 12R$$

$$i. t \leq 3$$

$$\text{當 } s_2 = i \cdots (i+t-1) \text{ 時, } \beta_q = 1 \quad \text{共有 } (i+t-1) - i + 1 = t \text{ 個 } 1$$

$$\text{當 } s_1 = (i+1) \cdots (i+t) \text{ 時, } \beta_q = 1 \quad \text{共有 } (i+t) - (i+1) + 1 = t \text{ 個 } 1$$

$$\text{所以 } \beta_q \text{ 有 } 2t \text{ 個 } 1 \Rightarrow d = 2 + 2t \geq 4$$

$$ii. t > 3$$

$$\text{當 } i = s_1 \cdots s_2 \text{ 時, } \beta_q = 1 \quad \text{共有 } s_2 - s_1 + 1 = 3 \text{ 個 } 1$$

$$\text{當 } i+t = s_1 \cdots s_2 \text{ 時, } \beta_q = 1 \quad \text{共有 } s_2 - s_1 + 1 = 3 \text{ 個 } 1$$

$$\text{所以 } \beta_q \text{ 有 } 6 \text{ 個 } 1 \Rightarrow \beta_i \text{ 有 } 12 - 12 \text{ 個 } 0 \Rightarrow d = 2 + 6 = 8$$

$$(2). i, i+t \in (12R+1) \sim (12R+4R)$$

$\therefore$ 每個 m 被 3 個 C 控制且每個 m 對應到的 c 均不重複

$$\therefore d = 2+6=8$$

$$(3). i, i+t \in (16R+1) \sim (16R+4R)$$

$\therefore$ 每個 m 被 3 個 C 控制且每個 m 對應到的 c 均不重複

$$\therefore d = 2+6=8$$

$$(4). i \in 1 \sim 12R, i+t \in (12R+1) \sim (12R+4R)$$

$\therefore \alpha_i$ 對應連續 3 個 $c, \alpha_{(i+t)}$ 對應到的 c 間隔 $4R$

$$\therefore d = \begin{cases} 2+4=6 \\ or \\ 2+6=8 \end{cases}$$

$$(5). i \in 1 \sim 12R, i+t \in (16R+1) \sim (16R+4R)$$

$\therefore \alpha_i$ 對應連續 3 個 $c, \alpha_{(i+t)}$ 對應到的 c 間隔 $2R$

$$i. \quad R=1 \Rightarrow d = \begin{cases} 2+2=4 \\ or \\ 2+4=6 \end{cases}$$

$$ii. \quad R \geq 2 \Rightarrow d = \begin{cases} 2+4=6 \\ or \\ 2+6=8 \end{cases}$$

$$(6). i \in (12R+1) \sim (12R+4R), i+t \in (16R+1) \sim (16R+4R)$$

$$\therefore i \equiv q \pmod{4R} \quad (i+t) \equiv q \pmod{2R}$$

$\therefore \beta$ 必不全相同

存在一個 β 只含 α_i , 不含 α_{i+t} , 且存在一個 β 只含 α_{i+t} , 不含 α_i

$$\text{故 } d \geq 2+2=4$$

$$3. \quad n(A) \geq 3 \Rightarrow n(B) \leq k-3$$

$$\text{令 } \alpha_i = 1, \alpha_j = 1, \alpha_k = 1$$

由 $n(A)=2$ 的結果可知： $\beta_q=1$ 的個數可能為 2 個、4 個或 6 個

先考慮 α_i, α_j 則

(1). $\beta_q = 1$ 的個數為 2 個

再考慮 α_k , 因為有三個 β_q 中含 α_k

所以若上面兩個 $\beta_q = 1$ 均被修正為 0, 則必有一 β_q 由 0 變為 1

若上面兩個 $\beta_q = 1$ 不全被修正為 0, 則至少有一個 $\beta_q = 1$

(2). $\beta_q = 1$ 的個數為 4 個

再考慮 α_k , 因為有三個 β_q 中含 α_k

上面四個 $\beta_q = 1$ 最多只有 3 個被修正為 0, 所以 $\beta_q = 1$ 的個數至少為 1

$$d \geq 4$$

由以上討論可知 $d_{\min} = 4$

伍、 研究結果

一、 由最小漢明距計算過程中得：一編碼法之 $d_{\min} \leq$ 生成矩陣 $d_{\min}$

$\Rightarrow$ 好的編碼方法需使其 $d_{\min} =$ 生成矩陣的 $d_{\min}$

二、 柏拉圖正多面體(正四面體、正六面體、正十二面體)編碼法之共通點

(一) 每個訊息碼 m 都被三個 c 檢測

最小漢明距皆為 4, 由 P22 的文獻： $s=2, t=1$, 可得每個字元內校正達 1 個誤差且偵測達 $2 > 1$ 個誤差 $d_{\min} \geq 1 + 2 + 1$

(二) 碼速隨著面個數增加而增加, 其碼速如下

$$1. \text{四面體編碼: } \frac{4}{8} = \frac{1}{2} \quad 2. \text{六面體編碼: } \frac{8}{14} = \frac{4}{7} \quad 3. \text{十二面體編碼: } \frac{20}{32} = \frac{5}{8}$$

三、 柏拉圖正多面體(正四面體、正六面體、正十二面體)編碼法之延伸

正四面體、正六面體及正十二面體的編碼皆可以依其訊息比次、檢查比次同乘 R 倍, 編碼的原則和原本的編碼方式相同, 其碼速和最小漢明距均維持不變。四面體編碼的延伸更可以依需要, 改變一個 c 控制的 m 的個數, 但在每個檢查碼 c 控制 l 個 m 中, 需 $l \geq 3$ 才能使得 $d_{\min} = 4$

四、 四面體編碼的延伸, 可以修正蜂窩編碼

若以 (n,k) $n=2k$ 編碼思考，蜂窩編碼的 $l=6-4=2 < 3 \therefore d_{\min}=1+l=1+2=3$

因此，如果要改善蜂窩編碼，只需要將一個 c 控制兩個 m 提升到 3 個 m 即可將其最小漢明距提升到 4。

五、 利用文獻中信種解碼的概念

利用信種解碼即可校對判斷單一誤差或判斷是否有雙重誤差

陸、 討論

在 (n,k) 線性區段碼時， m 有 k 個、 c 有 $n-k$ 個，每一個 c 及 m 的重要性均等。所以每一個 c 控制相同數目(l 個)的 m 且所有的 c 需涵蓋所有的 m ，每一個 m 需被相同數目(w 個) c 檢測。得 $l \cdot (n-k) = w \cdot k \quad l, n, k, w, (n-k) \in \mathbb{N}$

目前只推廣出 $(2R, R)$ $(14R, 8R)$ $(32R, 20R)$ 之編碼方式，未來可努力之方向可以利用上述(*)之條件式推廣至 (n,k) 的編碼方式。

柒、 結論

在我們發展出來的所有編碼法中，十二面體編碼法的最小漢明距為 4、碼速為 $\frac{5}{8}$ 為所有研究出的方法中最高，且這種編碼法更可以延伸到 $(32R, 20R)$ 的型態，所以我們認為十二面體編碼法為我們研究出的方法中之最佳。

捌、 參考資料及其他

一、文獻整理

(一) 誤差控制編碼(ERROR-CONTROL CODING)

1. 前言

數位通信系統中，在傳遞訊息時常因雜訊而造成誤差。為了追求精準無誤差，通常都加一些用來檢出誤差並校正的額外檢查位元。考量可靠度、效益性等狀況，所以因應各種需求設計不同誤差控制編碼。

2. 編碼法簡介

(1).同位檢查碼

方法：當一個字元，包含偶數個 1 時，我們稱此二進位字元為偶同位，含奇數個 1 的字元稱為奇同位。一種誤差偵測同位檢查碼的碼字是由 $n-1$ 個比次的訊息比次及一個檢查比次所構成。而此檢查比次的選擇是要使所有碼字皆有相同的同位。

例子：傳送訊息是 101，當我們接受到一個奇同位字元 001 時，便知有一個或三個誤差，通常說奇數個誤差。

優點：碼速高，可發現奇數個誤差。

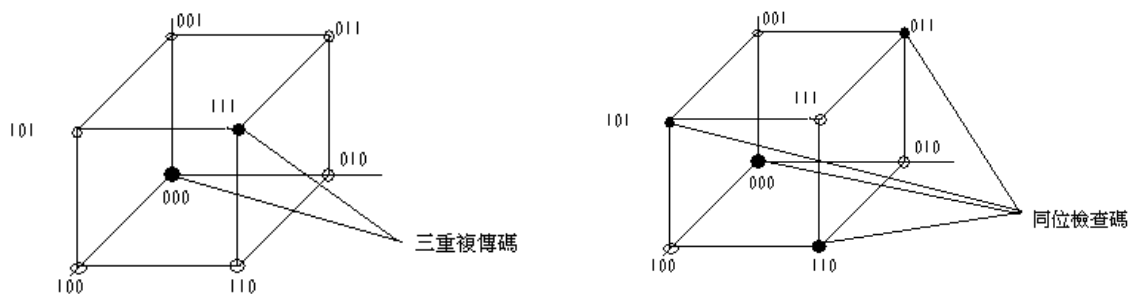
缺點：奇數個誤差狀況下，只可偵測有無誤差，但無法校對，且偶數個誤差所造成的有效同位亦無法偵測。

(2). 碼向量及漢明距

i. 碼向量

方法：以碼向量來表示，而非對某一特定碼的連續片段檢查。任一 n 位元比次的碼字皆可被看作一個 n 度空間之向量。而此向量之分量或座標等於碼字比次。

例子：碼字 101，以下列向量表示： $X = [1, 0, 1]$ 如圖是以三度空間的相關向量尖點來表示所有可能的 3 比次字碼。



ii. 漢明距

方法：兩個向量 X 、 Y 間的漢明距 $d[X, Y]$ 定義為相異分量的數目，而特定碼的最小距離 $d_{\min}$ 即為有效碼向量間的最小漢明距。

例子： $X = [1, 0, 1]$ ， $Y = [1, 1, 0]$ 則 $d[X, Y] = 2$ ，此乃因為其第二及第三分量相異之故。

優點：當一個碼字的傳輸誤差數目小於 $d_{\min}$ 時，誤差偵測是可能的。

缺點：當一個碼字的傳輸誤差數目大於 $d_{\min}$ 時，則誤差字元可能被認為是另一個有效向量而使其誤差無法被偵測出。

依此方式可導出對不同程度誤差控制概率的要求如下：

每個字元內偵測達 s 個誤差	$d_{\min} \geq s + 1$
校正達 t 個誤差	$d_{\min} \geq 2t + 1$
每個字元內校正達 t 個誤差且偵測達 $s > t$ 個誤差	$d_{\min} \geq t + s + 1$

(二) 線性區段碼(LINER BLOCK CODES)

1. 基本定義

(1) 碼向量的和：

假定有兩個區段碼其向量為 $X=(X_1 X_2 \dots X_n)$ ； $Z=(Z_1 Z_2 \dots Z_n)$

X 及 Z 中各分量為二進位數。則碼向量的和：

$$X+Z \triangleq (X_1 \oplus Z_1 \quad X_2 \oplus Z_2 \quad \dots \quad X_n \oplus Z_n)$$

在此我們先說明二元(binary)加法運算：

$$0 \oplus 0 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 1 \oplus 1 = 0$$

由上面四個式子可知： $a \oplus b = a - b$

(2) 碼的線性定義：該碼包括全零之向量，或任二個碼向量的和恰為該碼系統中另一向量。

說明： $X_i \in A, i \in R \quad X_1=(a_1, a_2, \dots, a_n) \quad X_2=(b_1, b_2, \dots, b_n) \quad X_1 \oplus X_2 = X_n$

$$\forall x, y \in A \Rightarrow x+y \in A$$

(3) 向量權(weight)：任一向量 X 中非零分量的數目，可記作 $w(X)$ ，稱為向量權。所以，任兩個碼向量 X 及 Z 間的漢明距為： $d(X, Z)=w(X+Z)$

即線性區段碼的最小漢明距為最小的非零向量權。

2. 方法

(1) 一種常用的區段碼常表示成： $X=(m_1 m_2 m_3 \dots m_k \quad c_1 c_2 c_3 \dots c_q)$

說明：共有 n 個比次。前 k 個向量為訊息比次，另外 $n-k$ 個〔或說後 q 個〕為檢查比次。為了方便，我們亦將此碼量寫成分段式的記號如右： $X=(M | C)$

說明：式中的 M 為一個 k 比次訊息向量， C 為一個 q 比次的檢查向量。

(2) 若 G 為 $k \times n$ 的產生矩陣 $G \triangleq [I_k | P]$ I_k 是 $k \times k$ 的單位矩陣(identity matrix)

$$P = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1q} \\ p_{21} & p_{22} & \cdots & p_{2q} \\ \vdots & \vdots & & \vdots \\ p_{k1} & p_{k2} & \cdots & p_{kq} \end{bmatrix} \dots \textcircled{1} \quad *P \text{ 為二進位數字的 } k \times q \text{ 副矩陣。則}$$

i. M 與 X 有下列關係： $X=MG$

說明：訊息向量 M 經產生矩陣的編碼後可產生一個 (n, k) 區段碼的碼向量 X 。

ii. 檢查碼 C 也可以用下列關係式來表達：

$C=MP$ C 的第 j 個分量是利用 P 的第 j 行來計算的。即

$$C_j = m_1 p_{1j} \oplus m_2 p_{2j} \oplus \dots \oplus m_k p_{kj} \quad j=1, 2, 3, \dots, q$$

3.優缺點

- (1) 優點：區段碼的矩陣表示法除了提供一種簡易的分析法外，亦可導出編碼器
- (2) 缺點：它並未告訴我們如何選取 P 子矩陣分量，所以無法確定如最小漢明距之類的參數。

我們將以漢明碼作例子來說明線性區段碼的應用。

4.漢明碼(Hamming codes)

(1)架構

漢明碼是一種 (n,k) 線性區段碼且其有 $q \geq 3$ 的檢查比次，同時 $n = 2^q - 1, k = n - q$

此碼的速率為： $R_c = \frac{k}{n} = 1 - \frac{q}{2^q - 1}$

所以，若 $q \gg 1$ 時 $R_c \approx 1$ 。最小距離為一固定值 3 且與 q 無關

(2)應用

∴每個字元內偵測達 s 個誤差

$$d_{\min} \geq s + 1$$

校正達 t 個誤差

$$d_{\min} \geq 2t + 1$$

每個字元內校正達 t 個誤差且偵測達 $s > t$ 個誤差

$$d_{\min} \geq t + s + 1$$

且 $d_{\min} = 3$ (7,4)漢明碼可用來校正單一誤差或偵測雙重誤差。欲構成一個常用的漢明碼，可使 P 子矩陣的 k 列組成全部的 q 比次字元(其可以任何順序排列，但至少要有兩個以上的 1)

(3)實例

考慮一種具有 $q=3$ 的常用漢明碼。可知 $n=2^3-1=7$ ； $k=7-3=4$

依前述規則，一個適當的生成矩陣為： $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$

由上式可知 $P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

假定有個區段訊息比次 $M=(m_1 \ m_2 \ m_3 \ m_4)$,其檢查比次可由下述方程式求得

$$c_1=m_1 \oplus m_2 \oplus m_3 \oplus 0$$

$$c_2=0 \oplus m_2 \oplus m_3 \oplus m_4$$

$$c_3=m_1 \oplus m_2 \oplus 0 \oplus m_4$$

其 $d_{\min}=3$

(三) 信種解碼(SYNDROME DECODING)

1.原理：假定 Y 代表特定向量 X 發送後接收到的向量，若 $X \neq Y$ 則表示有誤差被偵測出來，即可進行校正。

2.基本定義：

(1) 信種：一個 q 比次向量。例如： $(0,0,0)$ 為一個信種。

(2) 同位檢查矩陣：取一常用之 (n,k) 區段碼，若與其相關連的是一個 $q \times n$ 的

$$H \text{ 矩陣，則其同位檢查矩陣爲： } H^T \triangleq \left[\begin{array}{c} p \\ I_q \end{array} \right] \dots\dots\dots \textcircled{2}$$

H^T 為 H 的轉置矩陣； I_q 為 $q \times q$ 的單位矩陣。

其具有的特性爲： $XH^T=(00\dots0)$

3.方法

(1) 編碼：假設 X 屬於 (n,k) 區段碼向量集合的一個碼； Y 為一接收向量。
則具有下列特性

i. $XH^T=(00\dots0)$

ii. 其誤差檢出(error detection)爲： $S=YH^T$

所以若 $S=(00\dots0)$ 則表示

a. $Y=X$ 無誤差或誤差未檢出

b. $Y \neq X$ 有誤差被偵測出來，且 S 中非零之分量即表示被檢出之誤差。

(2) 解碼：

誤差校正可以以信種為基礎。所以可引進 n 比次的誤差向量 E (n -bit error vector E)的方法來發展解碼。此誤差向量的非零分量即標定 Y 中傳輸誤差的位置所在。 E 例： $X=(1 \ 0 \ 1 \ 1 \ 0)$; $Y=(1 \ 0 \ 0 \ 1 \ 1) \Rightarrow E=(0 \ 0 \ 1 \ 0 \ 1)$ ，可輕易看出第三個和第五個編碼有錯誤。

一般而言： $Y=X+E$ 。因為在同一比次位置的第二個誤差將可取消原來的誤差。將 $Y=X+E$ 帶入 $S=YH^T$ ，即可求：

$$S=(X+E)H^T = XH^T + EH^T = EH^T$$

討論單一誤差時，當 E 對應於一個碼字第 j 個比次的誤差，可由上式發現 S 即為 H^T 矩陣的第 j 列。

(3) 缺點：

i. 由於 2^n 個可能的 n 比次誤差向量所產生的信種僅有 2^q 種不同的情形(含無誤差)。因此，此種方法只可校正 2^q-1 個單一或更多誤差的型樣，同時其

餘的行樣為不可校正(uncorrectable)的。

- ii. 一個 n 比次的字元中，有 $\binom{n}{1}=n$ 個單一誤差的型樣， $\binom{n}{2}$ 個雙重誤差的型樣，依此類推。因此，如果以個碼每個字元的誤差校正達 t 個誤差比次時，其 q 及 n 必須滿足： $2^q-1 \geq n + \binom{n}{2} + \dots + \binom{n}{t}$

因為單一誤差的可能性大於雙重誤差的可能性，依此類推。所以，在單一誤差校正碼的特殊情形中，可簡化上式成 $2^q-1 \geq n$ 。對每個單一誤差及無誤差的型樣，我們都必須提供一不同的信種， H^T 的列必須全部不同且每個都必須至少包含一個非零向量。漢明碼的產生矩陣可設計成滿足 H 矩陣，然而 q 及 n 則必須滿足 $2^q-1=n$ 的形式。

4.舉例

利用上述方法解碼至單一誤差校正的(7,4)漢明碼系統上。

$$\text{由式②：} H^T \triangleq \begin{bmatrix} P \\ I_q \end{bmatrix} ; \text{式①} P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad *P \text{ 為前述之為二進位數字的 } k \times q \text{ 副矩陣}$$

$$\text{可求出一個 } 3 \times 7 \text{ 的同位檢查矩陣：} H = [P^T | I_q] = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

其共有 $2^3-1=7$ 個可校正個單一誤差型樣，同時其相對應的信種可直接由 H 矩陣的行而列於〈表一〉中。但是假設接收字元恰好有兩個誤差時，例如： $E=(1,0,0,0,0,1,0)$ 。解碼器計算 $S=YH^T=XH^T=(111)$ 。因此解碼輸出字元 $Y+\hat{E}$ 含有三個誤差：兩個傳輸誤差加上由解碼器引起的校正誤差。此時則會發生誤判的情形。

< 表一 >

S	$\hat{E}$
0 0 0	0 0 0 0 0 0 0
1 0 1	1 0 0 0 0 0 0
1 1 1	0 1 0 0 0 0 0
1 1 0	0 0 1 0 0 0 0
0 1 1	0 0 0 1 0 0 0
1 0 0	0 0 0 0 1 0 0
0 1 0	0 0 0 0 0 1 0
0 0 1	0 0 0 0 0 0 1

二、參考書籍

(一) A.Bruce.Carlson，湯鴻沼譯著(民 78)。信號與通訊。第 13 章 誤差控制編碼 (P584-P612)。全華科技圖書股份有限公司。

(二) 林福來等(民 92)。高中數學第四冊、數（甲）上冊、數（乙）下冊。南一書局。

三、附錄

c \ m	1	2	3	4	5	6	7	8
1	○				○	○	○	
2	○	○				○		○
3	○	○	○				○	
4		○	○	○				○
5			○	○	○		○	
6				○	○	○		○

表(一)

m c	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	○										○	○	○				○			
2	○	○										○		○				○		
3	○	○	○												○		○			
4		○	○	○												○		○		
5			○	○	○								○				○			
6				○	○	○								○				○		
7					○	○	○								○				○	
8						○	○	○								○				○
9							○	○	○				○						○	
10								○	○	○				○						○
11									○	○	○				○				○	
12										○	○	○				○				○

表(二)

中華民國第四十五屆中小學科學展覽會
評 語

高中組 數學科

040413

「碼」到成功

高雄市立高雄女子高級中學

評語：

1. 作品看來很像標準的密碼學教材。
2. 倘若添加實驗過程，必能凸顯其創新的意味。