第四屆旺宏科學獎

成果報告書

參賽編號：SA4-078

作品名稱：「碼」到成功

姓名：林筱涵

關鍵字：編碼、最小漢明距

摘　　要

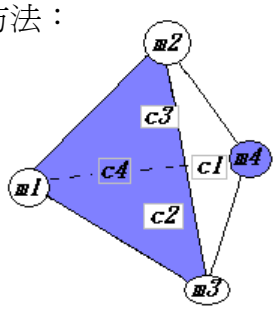
高一上地球科學講到太空時，突然想到：太空船傳回的資訊回到地球已經是很久以前的資料了，那麼如果傳送過程中受到干擾，接受到的資訊也可能是錯誤的。但是這些資料並不能複傳，所以必須有一種良好的傳輸方法，使我們能偵測並校正誤差。於是便開始研究：**在無複傳的狀況下，可校正誤差的編碼法**。

這個研究以柏拉圖多面體(正四、正六、正八、正十二及正二十面體)爲基礎發展不同的編碼方法：**以頂點對應訊息碼、面對應檢查碼**，由於正八面體及正二十面體頂點數目少於面的個數，所以不予討論。

針對(n,k)線性區段碼 X=(m_1 m_2 m_3...m_k c_1 c_2 c_3...c_{n-k})，一組訊息有 n 個比次。前 k 個分量爲訊息比次，另外 n-k 個爲檢查比次，我們發展出三個較好的編碼方法：

一、四面體編碼

如圖：m_x 爲訊息位元、c_x 爲檢查位元



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

碼速=$\frac{4}{8}$ ；最小漢明距($d_{\min}$)=4，即：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($k \geq 4, k \in \mathrm{N}$)的形式，其檢查碼定義爲：

$$c_q = m_1 \oplus m_2 \oplus \ldots \oplus m_k - m_{s_1} - m_{s_2} - \ldots - m_{s_i} \qquad q = 1 \sim k$$

$$q \equiv s_1 + i \equiv s_2 + (i-1) \equiv \cdots \equiv s_i + 1 \mod k \qquad s_1, s_2, \cdots, s_i \in \{1,2,3,\cdots,k\}$$

1.由於此種編碼法係由正四面體編碼的概念延伸而來，故在一組碼向量中訊息比次的個數要求需大於或等於 4。

2.若令每一個 c 檢測的訊息比次個數爲 l。則在 $l \geq 3$ 時可以做到碼速不變且 $d_{\min} = 4$；但在 $l = 2,1,0$ 時之 $d_{\min}$ 皆小於 4，意味著所能偵測及校正的功能下降，所以延伸時不考慮此種狀況。

3.延伸後的優點爲：每組碼向量的位元量和每個檢查比次 c 控制的訊息比次數目皆可依不同編碼需求做適當的調整，在一定的條件下，可以做到碼速及 $d_{\min}$ 均和正四面體編碼相同(碼速=$\frac{1}{2}$ 、$d_{\min} = 4$)。

二、六面體編碼

一個六面體會有 8 個頂點、六個面，所以這種編碼法爲一(14,8)之線性區段碼，每組訊息中含 8 個訊息比次、6 個檢查比次。檢查比次的定義如下：

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

$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \mod 6$, $q \equiv j \mod 2$ $j = 7,8$

此編碼 $d_{\min}$ =4，可偵測二個誤差且校正一個誤差，碼速=$\frac{8}{14}$。由六面體編碼法亦可推廣至(14R,8R) $R \in$ N 線性區段碼， $d_{\min}$ 及碼速均不變。

三、十二面體編碼

一個正十二面體有 20 個頂點、12 個面，所以此種編碼法每一組訊息皆有 20 個訊息比次、12 個檢查比次，爲一(32,20)線性區段碼。檢查碼的訊息如下：

$c_q = m_{s_1} \oplus m_{s_2} \oplus m_{s_3} \oplus m_j \oplus m_k$, $q = 1,2,3\cdots,12$, $s_1, s_2, s_3 \in \{1,2,3,\cdots,12\}$

$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \mod 12$, $q \equiv j \bmod 4$, $j = 13 \sim 16$

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

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。

我們得到的結果是：

1. 在柏拉圖多面體編碼法中，最小漢明距皆爲 4，碼速會隨著頂點個數的增加而增加。
2. 在正四面體、正六面體、正十二面體的基礎下，可以分別加以延伸出長度可調整之編碼。 $d_{\min}$ 和碼速都會和所對應到的正多面體相同。
3. 在整理的過程中，我們導出一個公式： $t \times (n-k) = w \times k$ 。一組碼向量中，訊息碼 m 有個 k 個、檢查碼 c 有 n-k 個。每一個 c 控制相同數目(t)個 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。

截至目前爲止，我們只發展出(2R,R)、(14R,8R)及(32R,20R)這三種線性區段碼，未來也許可經由上述的公式法展出碼速更高(即:傳出有效訊息比率更高)的編碼方法。

目　錄

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。於是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、 研究基礎

在研究過程中，我們利用線性區段碼的理論基礎設計出不同的編碼方法。因此，以下就線性區段碼作簡單的說明。

線性區段碼：假定有兩組編碼，其中每一組訊息皆看成一個向量，可表示爲

$X=(X_1 X_2...X_n)$ ； $Z=(Z_1 Z_2...Z_n)$，X 及 Z 中各分量爲二進位數。每一組區段碼可亦表示成：$X=(m_1 m_2 m_3...m_k c_1 c_2 c_3...c_q)$。共有 n 個比次，前 k 個向量爲訊息比次，另外 n-k 個〔或說後 q 個〕爲檢查比次。

若寫成分段式的記號如右：X=(M | C)，式中的 M 爲一個 k 比次訊息向量，C 爲一個 q 比次的檢查向量。

1. 碼向量的和： $X+Z \triangleq (X_1 \oplus Z_1 \quad X_2 \oplus Z_2 \ldots X_n \oplus Z_n)$。
   其中⊕爲二元(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爲該碼系統中另一向量。即： $X_i \in A, i \in R$ $X_1=(a_1, a_2,...,a_n)$ $X_2=(b_1,b_2,...,b_n)$ $X_1 \oplus X_2 = X_n$ 或者說： $\forall x,y \in A \Rightarrow x+y \in A$

3. 漢明距：兩個向量 X、Y 間的漢明距 d〔X,Y〕定義爲其相異分量的數目，而特定碼的最小距離 d_{min} 即爲有效碼向量間的最小漢明距。

   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；反之，當一個碼字的傳輸誤差數目大於或等於 d_{min} 時，則誤差字元可能被認爲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　$d_{min} \geq t+s+1$

4. 向量權(weight)：任一向量 X 中非零分量的數目，可記作 w(X)，稱爲向量權。所以,任兩個碼向量 X 及 Z 間的漢明距爲：d(X,Z)=w(X+Z)。即線性區段碼的最小漢明距爲最小的非零向量權。

5. 生成矩陣：若 G 爲 k×n 的生成矩陣 $G \triangleq [I_k \mid P]$　I_k 是 k×k 的單位矩陣；P 爲二進位數字的 k×q 副矩陣。　　$P=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1q} \\ p_{21} & p_{22} & \cdots & p_{2q} \\ \vdots & \vdots & & \vdots \\ p_{k1} & p_{k2} & \cdots & p_{kq} \end{bmatrix}$

則

i. 訊息碼 M 與 X 有下列關係：X=MG
   即：訊息向量 M 經生成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：
   $C_j=m_1p_{1j} \oplus m_2p_{2j} \oplus \ldots \oplus m_k p_{kj}$　　$j=1,2,3,\ldots,q$

伍、 研究過程

在研究過程中，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)。以頂點當作資料碼、面當作檢查碼。

因爲正八面體及正二十面體的頂點個數少於面的個數，碼速分別爲 $\frac{6}{14}$、$\frac{12}{32}$，小於 0.5，故不予討論。

一、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爲錯誤所在。

(1).訊息比次 m_x ：如圖 2。

(2).檢查碼 c_x：四面體中不包含 m_x 平面，如圖 2。

$C_1=m_2 \oplus m_3 \oplus m_4$

$C_2=m_1 \oplus m_3 \oplus m_4$

$C_3=m_1 \oplus m_2 \oplus m_4$

$C_4=m_1 \oplus m_2 \oplus m_3$

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

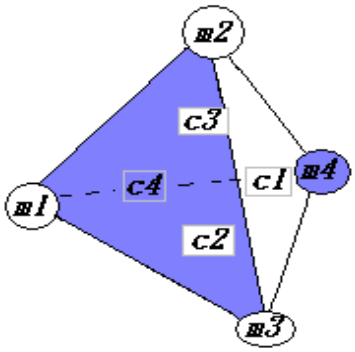
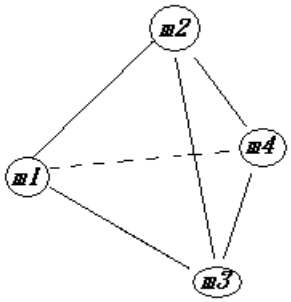


圖 2

2.生成矩陣

四面體編碼的生成矩陣如右：

$$G=\left[\begin{array}{cccc|cccc} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&1&1&0 \end{array}\right] = \left[M \quad \middle| \quad C\right]$$



M 爲 4×4 單位矩陣,C 爲單位矩陣所產生之檢查矩陣。任一列的 M 矩陣中其順序分別爲 $m_1m_2m_3m_4$ ；任一列的 C 矩陣中其順序分別爲 $c_1c_2c_3c_4$

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

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

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

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

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

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

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

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

$\therefore$ 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爲： $m_{11}m_{12}m_{13}m_{14}c_{11}c_{12}c_{13}c_{14}$

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

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： $m_{1p} \oplus m_{2p} = \alpha_p \qquad c_{1p} \oplus c_{2p} = \beta_p$ p=1,2,3,4

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

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

$\because \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \quad \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 = 1 \Rightarrow$ 4 個β中有 3 個 $1 \Rightarrow d = 1 + 3 = 4$

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

$\because \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \quad \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 = 0 \Rightarrow$ 4 個β中有 2 個 $1 \Rightarrow d = 2 + 2 = 4$

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

$\because \begin{cases} \alpha_i = 1 \\ \alpha_j = 0 \end{cases} \therefore \quad \alpha_1 \oplus \alpha_2 \oplus \alpha_3 \oplus \alpha_4 = 1 \Rightarrow$ 4 個β中有 1 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} 同爲 4。由研究基礎中漢明碼的(★)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

二、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爲 $m_1 m_2 \cdots m_k c_1 c_2 \cdots c_k$

m 爲訊息比次；c 爲檢查比次

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

$$q \equiv s_1 + i \equiv s_2 + (i-1) \equiv \cdots \equiv s_i + 1 \mod k \qquad s_1, s_2, \cdots, s_i \in \{1,2,3,\cdots,k\}$$

(二) 最小漢明距的計算過程

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

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

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

$A = \{i | \alpha_i = 1, i = 1,2,\cdots,k\}$ $B = \{j | \alpha_j = 0, j = 1,2,\cdots,k\}$, i≠j

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

$$q \equiv s_1 + i \equiv s_2 + (i-1) \equiv \cdots \equiv s_i + 1 \mod k \qquad s_1, s_2, \cdots, s_i \in \{1,2,3,\cdots,k\}$$

每個 β 中含 $k-i=l$ 個 α 以二元編碼運算相加。

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

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

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

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

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

(1). $t \le l$

當 $q+l-1 = i \cdots (i+t-1)$ 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 $\beta_q = 1$ 有 2t 個 1 $\Rightarrow d = 2+2t$

(2). $t > l$

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

當 $i+t = q \ldots (q+l-1)$ 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. $n(A) = 3 \Rightarrow n(B) = k-3$

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

$\because$ 每個 β 定義中 α 不完全相同且每個 α 平均對應在全部的 β 中

$\therefore$ 一定存在一個 β_q 其定義式中只含 $\alpha_i = 1, \alpha_j = 1, \alpha_k = 1$ 其中之一 $\Rightarrow d \ge 4$

由上述(1)(2)可得： $d \ge 4$

4. $n(A) \ge 4 \Rightarrow d \ge 4$

由 1.,2.,3.,4.,知：此種編碼之最小漢明距 $= \begin{cases} 1+l & l < 3 \\ 4 & l \ge 3 \end{cases}$

(三) 結果

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

再由文獻漢明碼的(★)： 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、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爲 $m_1m_2\cdots m_8c_1c_2\cdots c_6$

m 爲訊息比次；c 爲檢查比次

c 之定義爲：

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

$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \mod 6 \qquad , \; q \equiv j \mod 2 \quad j = 7,8$

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爲: $m_{11}m_{12}\cdots m_{18}c_{11}c_{12}\cdots c_{16}$

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

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

$$A = \{i | \alpha_i = 1, i = 1,2,3,\cdots,8\} \quad B = \{j | \alpha_j = 0, j = 1,2,3,\cdots,8\} \quad , \text{i} \neq \text{j}$$

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

$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \mod 6 \qquad q \equiv j \mod 2 \quad j = 7,8$

1. $n(A) = 1$

$\because$ 1 個 m 被三個 c 檢查 $\Rightarrow \alpha_q$ 可在三個不同的 β 中找到

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

2. $n(A) = 2$

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

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

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

i. $t \leq 3$

當 $s_3 = i \cdots (i+t-1)$ 時, $\beta_q = 1$　　共有 $(i+t-1)-i+1 = t$ 個 1

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

(註): $\beta_q = \alpha_{s_1} \oplus \alpha_{s_2} \oplus \alpha_{s_3} \oplus \alpha_{s_j}$

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

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

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

(3). $i \in C$　$j \in D$

i.若 i 爲奇數且 j 爲奇數

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 爲奇數且 j 爲偶數

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 爲偶數且 j 爲偶數

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 爲偶數且 j 爲奇數

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： $\beta_q = 1$ 的個數可能爲 2 個、4 個或 6 個

先考慮 α_i, α_j 則

(1). $\beta_q = 1$的個數爲 2 個

再考慮α_k,因爲有三個β_q中含α_k

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

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

(2). $\beta_q = 1$的個數爲 4 個

再考慮α_k,因爲有三個β_q中含α_k

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

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

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

由以上討論可得$d_{\min} = 4$

四、六面體編碼之延伸

(一)定義

一個(n,k)=(14R,8R),R∈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爲$m_1 m_2 \cdots m_{8R} c_1 c_2 \cdots c_{6R}$

m 爲訊息比次；c 爲檢查比次，c 之定義爲：

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

$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \mod 6R \quad q \equiv j \mod 2R, \quad j = 6R+1, 6R+2, \cdots, 8R$

(二) 最小漢明距的計算過程

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

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

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

$$A=\{i|\alpha_i=1,i=1,2,3,\cdots,8R\}\quad B=\{j|\alpha_j=0,j=1,2,3,\cdots,8R\}\ ,\ i\neq j$$

1. $n(A)=1$

∵每個 m 被三個 c 控制∴有三個$\beta=1$

$\Rightarrow d=1+3=4$

2. $n(A)=2$

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

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

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

i. $t\leq 3$

當$s_3=i\cdots(i+t-1)$時,$\beta_q=1$　　共有$(i+t-1)-i+1=t$個 1

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

所以β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). $i,v\in D$

∵檢查碼所檢查的訊息比次互斥∴$d=2+6=8$

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

∵α_i對應連續三個β,α_j對應到的β間隔 2R

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

$\Rightarrow n(A)=2$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： $\beta_q=1$的個數可能爲 2 個、4 個或 6 個

先考慮α_i,α_j則

(1). $\beta_q=1$的個數爲 2 個

再考慮α_k,因爲有三個β_q中含α_k

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

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

(2). $\beta_q=1$的個數爲 4 個

再考慮α_k,因爲有三個β_q中含α_k

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

由上述之(1)(2)$\Rightarrow d\geq 3+1=4$

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

綜合以上討論,可得$d_{\min}=4$

五、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爲$m_1m_2\cdots m_{20}c_1c_2\cdots c_{12}$，m 爲訊息比次；c 爲檢查比次

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

$$q\equiv s_1\equiv s_2+1\equiv s_3+2 \mod 12 \qquad q\equiv j \bmod 4,\ j=13\sim 16$$

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

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爲: $m_{11}m_{12}\cdots m_{1\,20}c_{11}c_{12}\cdots c_{1\,12}$

$m_{21}m_{22}\cdots m_{2\,20}c_{21}c_{22}\cdots c_{2\,12}$

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

$A=\{i|\alpha_i=1,i=1,2,\cdots,20\},B=\{j|\alpha_j=0,j=1,2,\cdots,20\}$ ，i ≠ j

1. $n(A)=1\Rightarrow n(B)=20-1=19\Rightarrow\beta$有 3 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. $t\le 3$

當 $s_3=i\cdots(i+t-1)$ 時, $\beta_q=1$ 共有 $(i+t-1)-i+1=t$ 個 1

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

所以β有 2t 個 $1\Rightarrow d=2+2t\ge 4$

ii. $t>3$

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

當 $i+t=q\ldots(q+3-1)$ 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). $i,i+t\in 13\sim 16$

∵每個 m 被 3 個 C 控制，且每個 m 對應到的 c 均不重複

$\Rightarrow$每個α對應到的β均不重複

$\therefore d=2+6=8$

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

∵每個 m 被 3 個 C 控制且每個 m 對應到的 c 均不重複

$\Rightarrow$每個α對應到的β均不重複

$\therefore d=2+6=8$

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

∵α_i對應連續 3 個β,α_j對應到的β間隔 4

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

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

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

$\therefore d=2+2=4 \quad or \quad 2+4=6 \quad or \quad 2+6=8$

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

α_i 對應到的 $\beta_q, i\equiv q \bmod 4$ ； α_{i+t} 對應到的 $\beta_q, (i+t)\equiv q \bmod 2$

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

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). $\beta_q=1$ 的個數爲 2 個

再考慮 α_k ,因爲有三個 β_q 中含 α_k

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

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

(2). $\beta_q=1$ 的個數爲 4 個

再考慮 α_k ,因爲有三個 β_q 中含 α_k

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

由上述(1)(2)可得 $d\geq 4$

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

由以上討論可知：最小漢明距爲 4

六、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爲 $m_1 m_2 \cdots m_{20R} c_1 c_2 \cdots c_{12R}$

m 爲訊息比次；c 爲檢查比次

c 之定義爲：

$$c_q = m_{s_1} \oplus m_{s_2} \oplus m_{s_3} \oplus m_j \oplus m_k \qquad q = 1,2,3,\cdots,12R \qquad s_1, s_2, s_3 \in \{1,2,3,\cdots,12R\}$$

$$q \equiv s_1 \equiv s_2 + 1 \equiv s_3 + 2 \bmod 12R \qquad q \equiv j \bmod 4R \;,\; j = (12R+1) \sim 16R$$

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

(二) 最小漢明距的計算過程：

假設有兩組訊息分別爲: $m_{11} m_{12} \cdots m_{1\,20R} c_{11} c_{12} \cdots c_{1\,12R}$

$m_{21} m_{22} \cdots m_{2\,20R} c_{21} c_{22} \cdots c_{2\,12R}$

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

$$A = \{i \,|\, \alpha_i = 1, i = 1,2,\cdots,20R\}, B = \{j \,|\, \alpha_j = 0, j = 1,2,\cdots,20R\} \text{ , i} \neq \text{j}$$

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

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

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

令 $\alpha_i, \alpha_{i+t} = 1$

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

i. $t \leq 3$

當 $s_3 = i \cdots (i+t-1)$ 時, $\beta_q = 1$ 共有 $(i+t-1) - i + 1 = t$ 個 1

當 $s_1 = (i+1) \cdots (i+t)$ 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$i = s_1, s_2, s_3$時, $\beta_q = 1$　　共有 3 個 1

當$i + t = s_1, s_2, s_3$時, $\beta_q = 1$　共有 3 個 1

所以β_q有6個 1$\Rightarrow \beta_i$有$12-12$個 0$\Rightarrow d = 2+6 = 8$

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

∵每個 m 被 3 個 C 控制且每個 m 對應到的 c 均不重複

$\Rightarrow$每個α對應到的β均不重複

$\therefore d = 2+6 = 8$

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

∵每個 m 被 3 個 C 控制且每個 m 對應到的 c 均不重複

$\Rightarrow$每個α對應到的β均不重複

$\therefore d = 2+6 = 8$

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

∵α_i對應連續 3 個β, $\alpha_{(i+t)}$對應到的β間隔 4R

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

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

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

i. R=1　$\Rightarrow d = 2+2 = 4$　*or*　$2+4 = 6$　*or*　$2+6 = 8$

ii. $R \geq 2$　$\Rightarrow d = 2+2 = 4$　*or*　$2+6 = 8$

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

∵$i \equiv q \bmod 4R$　$(i+t) \equiv q \bmod 2R$

$\therefore \beta$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

故$d \geq 2+2 = 4$

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

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

先考慮α_i,α_j則

(1). $\beta_q=1$的個數爲 2 個

再考慮α_k,因爲有三個β_q中含α_k

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

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

(2). $\beta_q=1$的個數爲 4 個

再考慮α_k,因爲有三個β_q中含α_k

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

$d\geq 4$

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

由 1.,2.,3.,4.可知$d_{\min}=4$

陸、 研究結果

一、由最小漢明距計算過程中得：一種編碼法之$d_{\min}$≤其生成矩陣$d_{\min}$

⇒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

最小漢明距皆爲 4，由文獻漢明碼的(★)可得：s=2,t=1,即每個字元內校正達 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

1.四面體編碼：$\frac{4}{8}=\frac{1}{2}$

2.六面體編碼：$\frac{8}{14}=\frac{4}{7}$

3.十二面體編碼：$\frac{20}{32}=\frac{5}{8}$

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似，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，需在 $l \geq 3$ 的條件下才能使得 $d_{\min} = 4$

在我們發展出來的所有編碼法中，正十二面體編碼法的最小漢明距爲 4、碼速爲 $\frac{5}{8}$，爲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；另一方面，正四面體編碼法的延伸雖然碼速只有 $\frac{1}{2}$，但每一組碼向量的個數相當有彈性。

在不同情況下對於傳輸資料會有不同的要求，所以在不同的情況下選擇最有利的編碼方法即爲最佳編碼！

柒、 討論

一、我們研究出的編碼方法，可應用在下列問題：

財團法人思源科技教育基金會 2005 年【數學專題】競賽題目

1 ~ 6 號六位役男的愛滋病檢測表及檢測結果

	1 號	2 號	3 號	4 號	5 號	6 號	檢測結果
檢測 一	取	取	取	不取	不取	不取	陽性
檢測 二	取	不取	不取	取	取	不取	陰性
檢測 三	不取	取	不取	取	不取	取	陰性
檢測 四	不取	不取	取	不取	取	取	陽性

假設有某一種昂貴的檢測劑可測量血液中是否有愛滋病毒： 當血液中有愛滋病毒時， 與此檢驗劑混合會呈陽性反應， 如果沒有病毒則會呈陰性反應。今假設兵役單位已抽取 1~ 6 號六位役男的血液備用。 未檢驗前已經知道此六位役男中最多只有一位感染愛滋病， 我們想知道是哪一位、或者根本六人都未染病。 如果以檢測劑一一測試六位役男的的血液， 則需要六劑檢測劑。 上表提供一種只要四劑就足夠測驗六人的方法。 這個方法每一次檢測一群人的混合血液，以檢測一爲例： 我們將 1 號、 2 號、 3 號 三人血液混合一起檢測， 其結果呈陽性， 所以顯示三人中有一人帶愛滋病毒。 檢測二取了 1 號、 4 號、 5 號而結果呈陰性，所以這三人都不帶病毒。 由以上兩檢測得知 2 號和 3 號其中必有一人帶愛滋病毒。 利用類似討論於檢測三， 也可排除 2 號感染的可能性， 所以 3 號是染愛滋病者。更詳細的討論可以知道不管哪一種檢測結果都可以知道哪一位染愛滋病。 以上四次的檢測是事先安排好以讓四次檢測同時進行， **我們要求不能參考檢測一的結果再決定檢測二時要檢測哪些人的混合血液**。

問題一: 假設已抽取 18 位役男的血液待測，且假設其中最多只有一位感染愛滋病。 試仿上表設計一種使用 t 個檢測劑就能成功的檢測表， 其中 $t < 18$ 且愈小愈好。 試將數字 18 換成任意自然數 n 而推廣你們的結果。

解決方法：

因爲要求使用的試劑 t<18 且越小越好，所以用碼速最高的正十二面體編碼法來解決。將每位役男看成一個訊息 m，有愛滋病的役男定義爲 $m=1$、健康者定義爲 $m=0$；試劑看成檢查碼 c。

因爲正十二面體編碼爲一(32,20)的區段碼，每個碼向量中會有 20 個訊息比次，所以在處理<問題一>時將 m_{19},m_{20} 的位置補上 0。而我們所能看到的是試劑檢測出的結果，也就是後面的檢查碼 c 的部分。題目中假設最多只有一位感染愛滋病，於是此組碼向量中最多只可能有一個 1。

假設此碼向量爲 $X=\left(M\middle|C\right)=\left(\underbrace{1000\cdots0}_{\text{共20個}}\middle|\underbrace{111000000000}_{\text{共12個}}\right)$。對照表二(正十二面體編碼對應圖)可知：$c_1,c_2,c_3$ 三者檢測到 m 的交集爲 m_1，且 $c_1=c_2=c_3=1$。於是可以確定 $m_1=1$、其餘皆爲 $0\Rightarrow$ 編號 1 號的役男感染了愛滋病。

所以利用正四面體、正六面體、正十二面體編碼法，即可解決若患有愛滋人數最多爲一人時，n 人檢測($n\geq4,n\in N$)的問題。這方法所需要試劑數量，或許不是最少，但仍是可行的方法。

二、 在研究過程中得到，(n,k)線性區段碼中，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)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 $l\bullet(n-k)=w\bullet k\quad l,n,k,w,(n-k)\in \mathrm{N}\cdots(*)$

目前只推廣出 $(2R,R)\quad(14R,8R)\quad(32R,20R)$ 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)線性區段碼的編碼方式。

捌、 參考資料及其他

一、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。

二、附錄

(一) 表格

說明：各欄及各列的數字代表編號 ex:第一欄第二列所對應到的是c_1

O 代表有對應到 ex:圖中的$c_1 = m_1 \oplus m_5 \oplus m_6 \oplus m_7$

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

表(一) 正六面體編碼對應圖

c \ m	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) 正十二面體編碼對應圖

(二) 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

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≠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：(000)爲一個信種。

(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×n 的

H 矩陣，則其同位檢查矩陣爲：$H^T \triangleq \left[\frac{p}{I_q}\right]$

H^T 爲 H 的轉置矩陣；I_q 爲 q×q 的單位矩陣。

其具有的特性爲：　　$XH^T=(00...0)$

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 爲一接收向量。

則具有下列特性

i. $XH^T=(00...0)$

ii. 其誤差檢出(error detection)爲：　$S=YH^T$

所以若 S=(00...0)則表示

a .Y=X　無誤差或誤差未檢出

b .Y≠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爲基礎。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。Ex：X=(1 0 1 1 0);Y=(1 0 0 1 1)⇒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。因爲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 $S=Y H^T$ ，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 即爲 H^T 矩陣的第 j 列。

所以我們可以利用信種解碼來判斷錯誤之訊息碼。