第 16 章

群、編碼理論，及 Polya 枚舉法

在我們的代數結構研究裡，我們檢視特殊的數學系統的性質。接著我們將我們的發現一般化，以便可研究和這些特別例子的共同潛在結構。

在第 14 章我們處理了環結構，其依賴兩個封閉的二元運算。現在我們轉到一個含有一個封閉二元運算的結構。這個結構叫做**群** (group)。

我們研究群將檢視許多和環類比的概念。然而，這裡我們主要集中在應用於密碼學、編碼理論，及一個由 George Polya 所創造的計數方法等所需的結構。

16.1 定義、例題，及基本性質

定義 16.1

若 G 是一個非空集合且 $\circ$ 是 G 上的一個二元運算，則稱 $(G, \circ)$ 是一個**群** (group) 若下面條件被滿足。

1) 對所有 $a, b \in G$，$a \circ b \in G$。 (G 在 $\circ$ 下的封閉性)
2) 對所有 $a, b, c \in G$，$a \circ (b \circ c) = (a \circ b) \circ c$。 (結合性質)
3) 存在 $e \in G$ 滿足 $a \circ e = e \circ a = a$，對所有 $a \in G$。(單位元素的存在)
4) 對每個 $a \in G$，存在 $b \in G$ 使得 $a \circ b = b \circ a = e$。(反元素的存在)

更而，若 $a \circ b = b \circ a$ 對所有 $a, b \in G$，則稱 G 是一個**交換** (commutative or abelian) 群。形容詞**交換** (abelian) 是紀念挪威數學家 Niels

Henrik Abel (1802-1829)。

我們瞭解定義 16.1 的第一個條件可被省略若我們僅需要 G 的二元運算是一個**封閉的** (closed) 二元運算。

在定義 14.1 (對一個環) 之後，我們提過＋(環加法) 及・(環乘法) 的封閉二元運算的結合律如何可以數學歸納法來擴充。同樣情形出現給群。若 $(G, \emptyset)$ 是任一群，且 r，$n \in \mathbf{Z}^+$，其中 $n \geq 3$ 且 $1 \leq r < n$，則

$$(a_1 \circ a_2 \circ \cdots \circ a_r) \circ (a_{r+1} \circ \cdots \circ a_n) = a_1 \circ a_2 \circ \cdots \circ a_r \circ a_{r+1} \circ \cdots \circ a_n,$$

其中 a_1，a_2，…，a_r，a_{r+1}，…，a_n 均是 G 的元素。

例題 16.1

在尋常的加法下，$\mathbf{Z}$，$\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$ 每一個均是一個交換群。它們之中沒有一個在乘法之下是一個群，因為 0 沒有乘法反元素。然而 $\mathbf{Q}^*$，$\mathbf{R}^*$，及 $\mathbf{C}^*$ (分別為 $\mathbf{Q}$，$\mathbf{R}$，及 $\mathbf{C}$ 的所有非零元素所成之集合) 在尋常的乘法之下是交換群。

若 $(R, +, \cdot)$ 是一個環，則 $(R, +)$ 是一個交換群；**體** (field) $(F, +, \cdot)$ 的所有非零元素形成交換群 $(F^*, \cdot)$。

例題 16.2

對 $n \in \mathbf{Z}^+$，$n > 1$，我們發現 $(\mathbf{Z}_n, +)$ 是一個交換群。當 p 是一個質數，$(\mathbf{Z}^*_p, \cdot)$ 是一個交換群。表 16.1 及 16.2 分別說明 $n = 6$ 及 $p = 7$ 的情形。(記得在 $\mathbf{Z}_n$，我們經常以 a 表 $[a] = \{a + kn | k \in \mathbf{Z}\}$。相同的記號被使用於 $\mathbf{Z}^*_p$。)

表 16.1

＋	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

表 16.2

・	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

定義 16.2

對每個 G，G 的元素個數被稱是 G 的**階數** (order) 且被表為 $|G|$。當 G 的元素個數不是有限時，我們稱 G 有無限階數。

對所有 $n \in \mathbf{Z}^+$，$|(\mathbf{Z}_n, +)| = n$，而 $|(\mathbf{Z}^*_p, \cdot)| = p - 1$ 對每個質數 p。

例題 16.3

例題 16.4

讓我們以環 $(\mathbf{Z}_9, +, \cdot)$ 開始且考慮子集合 $U_9 = \{a \in \mathbf{Z}_9 | a$ 是 $\mathbf{Z}_9$ 的可逆元素$\} = \{a \in \mathbf{Z}_9 | a^{-1}$ 存在$\} = \{1, 2, 4, 5, 7, 8\} = \{a \in \mathbf{Z}^+ | 1 \le a \le 8$ 且 $\gcd(a, 9) = 1\}$。表 16.3 告訴我們 U_9 在環 $(\mathbf{Z}_9, +, \cdot)$ 的乘法下是封閉——即乘法模 9。更而，我們亦看到 1 是單位元素且每個元素有一個反元素 (在 U_9)。例如，5 是 2 的反元素，且 7 是 4 的反元素。最後，因為每個環在 (環) 乘法運算下是可結合的，所以 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$，對所有 a，b，$c \in U_9$。因此，$(U_9, \cdot)$ 是一個階數為 6 的群——它是一個階數為 6 的交換群。

表 16.3

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

一般來講，對每個 $n \in \mathbf{Z}^+$，其中 $n > 1$，若 $U_n = \{a \in (\mathbf{Z}_n, +, \cdot) | a$ 是一個可逆元素$\} = \{a \in \mathbf{Z}^+ | 1 \le a \le n - 1$ 且 $\gcd(a, n) = 1\}$，則 $(U_n, \cdot)$ 在 (封閉的) 模 n 的乘法二元運算下是一個交換群。群 $(U_n, \cdot)$ 被稱是環 $(\mathbf{Z}_n, +, \cdot)$ 的**可逆元素群** (group of units)，且它的階數為 $\phi(n)$，其中 ϕ 表 8.1 節的 Euler phi 函數。

從現在開始，群運算將被寫為乘法，除非它被給為其它類型。所以 $a \not\cdot b$ 現在變為 ab。

下面定理提供幾個所有群共享的性質。

對每個群 G，

定理 16.1

a) G 的單位元素是唯一的。

b) G 的每個元素的反元素是唯一的。

c) 若 a，b，$c \in G$ 且 $ab = ac$，則 $b = c$。 (左邊-消去性質)

d) 若 a，b，$c \in G$ 且 $ba = ca$，則 $b = c$。 (右邊-消去性質)

證明：

a) 若 e_1，e_2 均為 G 的單位元素，則 $e_1 = e_1e_2 = e_2$。(驗證每個等號。)
b) 令 $a \in G$ 且假設 b，c 均為 a 的反元素，則 $b = be = b(ac) = (ba)c = ec = c$。(驗證每個等號。)

性質 (c) 和 (d) 的證明留給讀者。(由於這些性質，我們發現一個有限群表，表中每個群元素在各列及各行中恰出現一次。)

基於定理 16.1(b) 的結果，a 是唯一反元素，將被指定為 a^{-1}。當群被寫為相加，$-a$ 被用來表示 a 的 (加法) 反元素。

如同乘法在環的情形，我們有元素的冪次方於群裡。我們定義 $a^0 = e$，$a^1 = a$，$a^2 = a \cdot a$，且一般來講，$a^{n+1} = a^n \cdot a$，對所有 $n \in \mathbf{N}$。因為每個群元素有一個反元素，對 $n \in \mathbf{Z}^+$，我們定義 $a^{-n} = (a^{-1})^n$。則 a^n 被定義對所有 $n \in \mathbf{Z}$，且可證明對所有 m，$n \in \mathbf{Z}$，$a^m \cdot a^n = a^{m+n}$ 且 $(a^m)^n = a^{mn}$。

若群運算是加法，則以倍數代替冪次方，且對所有 m，$n \in \mathbf{Z}$，及所有 $a \in G$，我們發現

$$ma + na = (m + n)a \quad m(na) = (mn)\,a.$$

此時單位元素被表為 0，而非 e。且在這裡，對所有 $a \in G$，我們有 $0a = 0$，其中 a 前面的“0”是整數 0 (在 $\mathbf{Z}$ 上) 而等式右邊的“0”是單位元素的 0 (在 G 上)。[所以這兩個“0”是不同的。]

對一個交換群 G，我們亦發現對所有 $n \in \mathbf{Z}$ 且所有 a，$b \in G$，(1) $(ab)^n = a^nb^n$，當 G 被寫為相乘時；且 (2) $n(a + b) = na + nb$，當加法運算被使用於 G 時。

我們現在看看群的一個特別子集合。

例題 16.5

令 $G = (\mathbf{Z}_6, +)$。若 $H = \{0, 2, 4\}$，則 H 是 G 的一個非空子集合。表 16.4 證明 $(H, +)$ 在 G 的二元運算下亦是一個群。

表 16.4

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

此情形引出下面定義。

定義 16.3

令 G 是一個群且 $\emptyset \neq H \subseteq G$。若 H 在 G 的二元運算下是一個群，則我們稱 H 是 G 的一個**子群** (subgroup)。

例題 16.6

a) 每個群 G 有 $\{e\}$ 和 G 做為子群。它們是 G 的**明顯** (trivial) 子群。所有其它子群被叫做**非明顯** (nontrivial) 子群，或**眞** (proper) 子群。

b) 除了 $H=\{0, 2, 4\}$ 外，子集合 $K=\{0, 3\}$ 亦是 $G=(\mathbf{Z}_6, +)$ 的一個(真)子群。

c) 非空子集合 $\{1, 8\}$ 和 $\{1, 4, 7\}$ 均是 $(U_9, \cdot)$ 的子群。

d) 群 $(\mathbf{Z}, +)$ 是 $(\mathbf{Q}, +)$ 的一個子群，而 $(\mathbf{Q}, +)$ 是 $(\mathbf{R}, +)$ 的一個子群。但 $\mathbf{Z}^*$ 在乘法之下不是 $(\mathbf{Q}^*, \cdot)$ 的子群。(為何不是？)

對一個群 G 及 $\emptyset \neq H \subseteq G$，下面告訴我們何時 H 是 G 的一個子群。

定理 16.2

若 H 是群 G 的非空子集合，則 H 是 G 的子群若且唯若 (a) 對所有 $a, b \in H$，$ab \in H$，(b) 對所有 $a \in H$，$a^{-1} \in H$。

證明：若 H 是 G 的子群，則由定義 16.3，H 在相同二元運算下是一個群。因此，它滿足所有的群條件，包含這裡所提的兩個。反之，令 $\emptyset \neq H \subseteq G$ 且 H 滿足條件 (a) 和 (b)。對所有 $a, b, c \in H$，$(ab)c=a(bc)$ 於 G 上，所以 $(ab)c=a(bc)$ 於 H 上(我們稱 H "繼承" G 的結合性質)。最後，因 $H \neq \emptyset$，令 $a \in H$。由條件 (b)，$a^{-1} \in H$ 且由條件 (a)，$aa^{-1}=e \in H$，所以 H 含有單位元素且是一個群。

一個有限條件修正情況。

定理 16.3

若 G 是一個群且 $\emptyset \neq H \subseteq G$，且 H **有限** (finite)，則 H 是 G 的子群若且唯若 H 在 G 的二元運算下是封閉的。

證明：如在定理 16.2 的證明，若 H 是 G 的子群，則 H 在 G 的二元運算下是封閉的。反之，令 H 是 G 的一個有限非空子集合且是封閉的。若 $a \in H$，則 $aH=\{ah | h \in H\} \subseteq H$，因為封閉條件。由 G 的左邊消去律，$ah_1=ah_2 \Rightarrow h_1=h_2$，所以 $|aH|=|H|$。因為 $aH \subseteq H$ 且 $|aH|=|H|$，由 H 是有限的得 $aH=H$。因 $a \in H$，存在 $b \in H$ 滿足 $ab=a$。但 (在 G) $ab=a=ae$，所以，$b=e$ 且 H 含有單位元素。因 $e \in H=aH$，存在元素 $c \in H$ 使得 $ac=e$。則 $(ca)^2=(ca)(ca)=(c(ca))a=(ce)a=ca=(ca)e$，所以 $ca=e$，且 $c=a^{-1} \in H$。因此，由定理 16.2，H 是 G 的子群。

定理 16.3 的有限條件是決定性的。$\mathbf{Z}^+$ 和 $\mathbf{N}$ 兩者均是群 $(\mathbf{Z}, +)$ 的非空封閉子集合，但兩者中沒有一個有群結構所需的加法反元素。

下一個例題提供一個非交換群。

例題 16.7

考慮圖 16.1(a) 所示的第一個等邊三角形。當我們對與三角形所在的平面垂直且通過三角形中心 C 的軸，以逆時針方向 (在三角形所在的平面) 旋轉這個三角形 120° 時，我們得到圖 16.1(a) 所示的第二個三角形。所以，圖 16.1(a) 中原來標示 1 的頂點現在位在原先標示 3 的位置。同樣的，2 現在位在原先 1 所佔的位置，且 3 移至原先 2 的位置。此可由函數 $\pi_1 : \{1, 2, 3\} \to \{1, 2, 3\}$ 來描述，其中 $\pi_1(1) = 3$，$\pi_1(2) = 1$，$\pi_1(3) = 2$。一個更緊緻的記法 $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$，其中我們記 $\pi_1(i)$ 為 i 之下的值，對每個 $1 \le i \le 3$，強調 π_1 是 $\{1, 2, 3\}$ 的一個排列。若 π_2 表逆時針旋轉 240°，則 $\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$。對單位元素 π_0 ——亦即，旋轉 $n(360°)$，其中 $n \in \mathbf{Z}$ ——我們記 $\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$。這些旋轉被稱是三角形的**剛體運動** (rigid motions)。它們是二-維運動，其保持中心 C 固定且保留三角形的形狀。因此，三角形看起來和我們剛開始的相同，除了某些頂點上標示的可能重排。

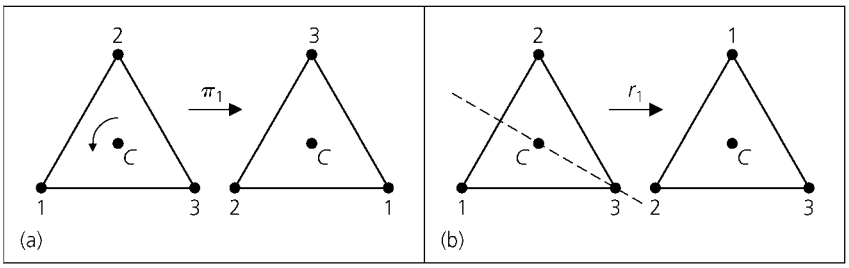


圖 16.1

除了這些旋轉外，三角形可沿著一條通過一頂點及其對邊中點的軸做鏡射。對平分右邊底角的軸，鏡射給了圖 16.1(b) 的結果。我們將這個表為 $r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$。對平分左邊底角的軸，相似的鏡射產生排列 $r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$。當三角形對其垂直軸做鏡射時，我們有 $r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$。每個 r_i，其中 $1 \le i \le 3$，是一個三-維的剛體運動。

令 $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$，即等邊三角形剛體運動 (在空間) 所成的集合。我們定義剛體運動 $\alpha\beta$，其中 $\alpha, \beta \in G$，為先做 α 接著再做 β 後所得的剛體運動。因此，例如，$\pi_1 r_1 = r_3$。我們可以幾何觀點來看這個，但考慮排列如下將更為方便：$\pi_1 r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$，其中，例如，$\pi_1(1) = 3$ 及 $r_1(3) = 3$，且我們記 $1 \xrightarrow{\pi_1} 3 \xrightarrow{r_1} 3$。所以 $1 \xrightarrow{\pi_1 r_1} 3$ 在乘積 $\pi_1 r_1$ 裡。

(注意我們這裡所寫的乘積 $\pi_1 r_1$ 之順序和在 5.6 節所定義的合成函數之順序相反。5.6 節的記法發生在分析裡，而在代數裡有傾向使用這個相反順序。) 而且，因為 $2 \xrightarrow{\pi_1} 1 \xrightarrow{r_1} 2$ 且 $3 \xrightarrow{\pi_1} 2 \xrightarrow{r_1} 1$，得 $\pi_1 r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_3$。

表 16.5 證明在這個二元運算下，G 是封閉的，且具單位元素 π_0。而且 $\pi_1{}^1 = \pi_2$，$\pi_2{}^1 = \pi_1$，且每個其它元素是自己的反元素。因為 G 的所有元素確實是函數，由定理 5.6，結合性質成立 (雖然以相反順序)。

表 16.5

$\cdot$	π_0	π_1	π_2	r_1	r_2	r_3
π_0	π_0	π_1	π_2	r_1	r_2	r_3
π_1	π_1	π_2	π_0	r_3	r_1	r_2
π_2	π_2	π_0	π_1	r_2	r_3	r_1
r_1	r_1	r_2	r_3	π_0	π_1	π_2
r_2	r_2	r_3	r_1	π_2	π_0	π_1
r_3	r_3	r_1	r_2	π_1	π_2	π_0

我們計算出 $\pi_1 r_1$ 為 r_3，但由表 16.5，我們看到 $r_1 \pi_1 = r_2$。由於 $\pi_1 r_1 = r_3 \neq r_2 = r_1 \pi_1$，得 G 是非交換的。

此群亦可得到為集合 {1, 2, 3} 的所有排列在函數合成的二元運算下所成的群。它被表為 S_3 (三個符號的**對稱** (symmetric) 群)。

例題 16.8

對稱群 S_4 是 {1, 2, 3, 4} 的 24 個排列所組成的。此處 $\pi_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ 是單位元素。若 $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$，$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$，則 $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$，但 $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$，所以 S_4 是非交換的。而且 $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ 且 $\alpha^2 = \pi_0 = \beta^3$。$S_4$ 有一個階數為 8 的子群，其為表示一個正方形之剛體運動的群。

我們現在轉到由較小群得到較大群的結構。

定理 16.4

令 $(G, \circ)$ 及 $(H, *)$ 為群。定義 $G \times H$ 上的二元運算為 $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$。則 $(G \times H, \cdot)$ 是一個群且被稱是 G 和 H 的**直積** (direct product)。

證明：$(G \times H, \cdot)$ 的群性質之證明留給讀者。

例題 16.9

考慮群 $(\mathbf{Z}_2, +)$，$(\mathbf{Z}_3, +)$。在 $G = \mathbf{Z}_2 \times \mathbf{Z}_3$ 上，定義 $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$，則 G 是一個階數為 6 的群，其中單位元素是 (0, 0)，且

例如，元素 (1, 2) 的反元素是 (1, 1)。

習題 16.1

1. 對下面各個集合，決定在所敘述的二元運算下，是否為一個群。若是，決定其單位元素及其每個元素的反元素。若它不是一個群，敘述它不滿足的定義條件。
   a) $\{-1, 1\}$ 在乘法下。
   b) $\{-1, 1\}$ 在加法下。
   c) $\{-1, 0, 1\}$ 在加法下。
   d) $\{10n | n \in \mathbf{Z}\}$ 在加法下。
   e) 所有一對一函數 $g : A \to A$ 所成的集合，其中 $A = \{1, 2, 3, 4\}$，在函數合成下。
   f) $\{a/2^n | a, n \in \mathbf{Z}, n \geq 0\}$ 在加法下。
2. 證明定理 16.1 的 (c) 和 (d)。
3. 為何集合 $\mathbf{Z}$ 在減法下不是一個群？
4. 令 $G = \{q \in \mathbf{Q} | q \neq -1\}$。定義 G 上的二元運算 $\emptyset$ 為 $x \emptyset y = x + y + xy$。證明 $(G, \emptyset)$ 是一個交換群。
5. 定義 $\mathbf{Z}$ 上的二元運算 $\emptyset$ 為 $x \emptyset y = x + y + 1$，證明 $(\mathbf{Z}, \emptyset)$ 是一個交換群。
6. 令 $S = \mathbf{R}^* \times \mathbf{R}$。定義 S 上的二元運算 $\emptyset$ 為 $(u, v) \emptyset (x, y) = (ux, vx + y)$。證明 $(S, \emptyset)$ 是一個非交換群。
7. 找群 U_{20} 及 U_{24} 的所有元素，U_{20} 及 U_{24} 分別為環 $(\mathbf{Z}_{20}, +, \cdot)$ 及 $(\mathbf{Z}_{24}, +, \cdot)$ 的可逆元素所成的群。
8. 對任意群 G，證明 G 是交換的若且唯若 $(ab)^2 = a^2b^2$ 對所有 $a, b \in G$。
9. 若 G 是一個群，證明對所有 $a, b \in G$。
   (a) $(a^{-1})^{-1} = a$　　(b) $(ab)^{-1} = b^{-1}a^{-1}$
10. 證明群 G 是交換的若且唯若對所有 $a, b \in G$，$(ab)^{-1} = a^{-1}b^{-1}$。
11. 求下面各個群的所有子群。
    (a) $(\mathbf{Z}_{12}, +)$　　(b) $(\mathbf{Z}_{11}^*, \cdot)$　　(c) S_3
12. a) 一個正方形有多少個 (2-維或3-維的) 剛體運動？
    b) 像表 16.5 給等邊三角形一樣，製造一個群表給這些剛體運動。這個群的單位元素是什麼？以幾何觀點描述各個元素的反元素。
13. a) 一個正五邊形有多少個 (2-維或3-維的) 剛體運動？以幾何觀點描述它們。
    b) 對一個正 n 邊形，$n \geq 3$，回答 (a)。
14. 在群 S_5 中，令
    $$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \text{ 及 } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$
    決定 $\alpha\beta$, $\beta\alpha$, α^3, β^4, α^{-1}, β^{-1}, $(\alpha\beta)^{-1}$, $(\beta\alpha)^{-1}$ 及 $\beta^{-1}\alpha^{-1}$。
15. 若 G 是一個群，令 $H = \{a \in G | ag = ga$ 對所有 $g \in G\}$。證明 H 是 G 的子群。(這個子群 H 被稱是 G 的**核** (center)。)
16. 令 ω 是複數 $(1/\sqrt{2})(1 + i)$。
    a) 令 $\omega^8 = 1$，但 $\omega^n \neq 1$ 對 $n \in \mathbf{Z}^+$，$1 \leq n \leq 7$。
    b) 證明 $\{\omega^n | n \in \mathbf{Z}^+, 1 \leq n \leq 8\}$ 在乘法下是一個交換群。
17. a) 證明定理 16.4。
    b) 將定理 16.4 及例題 16.9 所發展的概念擴大至群 $\mathbf{Z}_6 \times \mathbf{Z}_6 \times \mathbf{Z}_6 = \mathbf{Z}_6^3$，回答下

面問題。

i) 這個群的階數是多少？

ii) 找一個階數為 6 的 $\mathbf{Z}_6^3$ 之子群，一個階數為 12 的 $\mathbf{Z}_6^3$ 之子群，及一個階數為 36 的 $\mathbf{Z}_6^3$ 之子群。

iii) 求 (2, 3, 4)，(4, 0, 2)，(5, 1, 2) 各個元素的反元素。

18. a) 若 H，K 是群 G 的子群，證明 $H \cap K$ 亦是 G 的子群。

b) 給一個群 G 及其子群 H，K 使得 $H \cup K$ 不是 G 的子群的例子。

19. a) 求 $(\mathbf{Z}_5^*, \cdot)$ 上的所有 x 滿足 $x = x^{-1}$。

b) 求 $(\mathbf{Z}_{11}^*, \cdot)$ 上的所有 x 滿足 $x = x^{-1}$。

c) 令 p 為一質數。求 $(\mathbf{Z}_P^*, \cdot)$ 上的所有 x 滿足 $x = x^{-1}$。

d) 證明 $(p-1)! \equiv -1 \pmod{p}$，其中 p 為一質數。[此為著名的 Wilson 定理，雖然 John Wilson (1741-1793) 只是猜測它。第一個證明由 Joseph Louis Lagrange (1736-1813) 給於 1770 年。

20. a) 求 $(U_8, \cdot)$ 上的 x，其中 $x \neq 1$，$x \neq 7$ 但 $x = x^{-1}$。

b) 求 $(U_{16}, \cdot)$ 上的 x，其中 $x \neq 1$，$x \neq 15$ 但 $x = x^{-1}$。

c) 令 $k \in \mathbf{Z}^+$，$k \geq 3$。求 $(U_{2^k}, \cdot)$ 上的 x，其中 $x \neq 1$，$x \neq 2^k - 1$ 但 $x = x^{-1}$。

16.2　同態函數、同構函數，及循環群

我們再次將我們的注意力轉到保留結構的函數。

例題 16.10

令 $G = (\mathbf{Z}, +)$ 及 $H = (\mathbf{Z}_4, +)$。定義 $f: G \to H$ 為

$$f(x) = [x] = \{x + 4k | k \in \mathbf{Z}\}.$$

對所有 x，$y \in G$,

$$f(x+y) = [x+y] = [x] + [y] = f(x) + f(y),$$

($+$ 上方：G 上的運算；$+$ 下方：H 上的運算)

其中第二個等號由 14.3 節所發展的等價類加法得到。因此，此處之 f 保留群運算，且 f 是一個我們現在將定義的特殊型態函數的例子。

定義 16.4

若 $(G, \lozenge)$ 及 $(H, *)$ 是群且 $f: G \to H$，則 f 是一個**群同態函數** (group homomorphism)，若對所有 a，$b \in G$，$f(a \lozenge b) = f(a) * f(b)$。

當我們知道所給的結構是群時，函數 f 被稱為同態函數。
同態函數的一些性質被給在下面定理裡。

定理 16.5

令 $(G, \emptyset)$，$(H, *)$ 為分別具有單位元素 e_G，e_H 的群。若 $f: G \to H$ 是一個同態函數，則

a) $f(e_G) = e_H$
b) $f(a^{-1}) = [f(a)]^{-1}$ 對所有 $a \in G$
c) $f(a^n) = [f(a)]^n$ 對所有 $a \in G$ 及所有 $n \in \mathbf{Z}$。
d) $f(S)$ 是 H 的一個子群對 G 的每一個子群 S。

證明：

a) $e_H * f(e_G) = f(e_G) = f(e_G \emptyset\ e_G) = f(e_G) * f(e_G)$，所以由 [定理 16.1(d) 的] 右邊-消去律，得 $f(e_G) = e_H$。
b) & c) 兩部份的證明留給讀者。
d) 若 S 是 G 的一個子群，則 $S \neq \emptyset$，所以 $f(S) \neq \emptyset$。令 $x, y \in f(S)$，則 $x = f(a)$，$y = f(b)$，對某些 $a, b \in S$。因為 S 是 G 的一個子群，得 $a \emptyset b \in S$，所以 $x * y = f(a) * f(b) = f(a \emptyset b) \in f(S)$。最後，$x^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(S)$，因為 $a^{-1} \in S$ 當 $a \in S$。因此，由定理 16.2，$f(S)$ 是 H 的一個子群。

定義 16.5

若 $f: (G, \emptyset) \to (H, *)$ 是一個同態函數，我們稱 f 是一個**同構函數** (isomorphism) 若 f 是一對一且映成。此時，G，H 被稱是**同構群** (isomorphic groups)。

例題 16.11

令 $f: (\mathbf{R}^+, \cdot) \to (\mathbf{R}, +)$，其中 $f(x) = \log_{10}(x)$。此函數既是一對一且映成。 (證明這些性質。) 對所有 $a, b \in \mathbf{R}^+$，$f(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = f(a) + f(b)$。因此，$f$ 是一個同構函數，且正實數在乘法之下的群抽象等同於所有實數在加法之下的群。此處之函數 f 將實數的乘法問題 (不使用計算器會有一些困難) 轉換至一個處理實數加法的問題 (一個較簡單的算術考量。) 這是在計算器方便之前，使用對數背後的主要理由。

例題 16.12

令 G 為複數 $\{1, -1, i, -i\}$ 在乘法下的群。表 16.6 說明這個群的乘法表。以 $H = (\mathbf{Z}_4, +)$，考慮 $f: G \to H$ 定義為

$$f(1) = [0] \quad f(-1) = [2] \quad f(i) = [1] \quad f(-i) = [3].$$

則 $f((i)(-i))=f(1)=[0]=[1]+[3]=f(i)+f(-i)$，且 $f((-1)(-i))=f(i)$
$=[1]=[2]+[3]=f(-1)+f(-i)$.

雖然我們沒有檢查所有可能情形，但這個函數是一個同構函數。注意 G 的子群 $\{1, -1\}$ 在 f 之下的像是 $\{[0], [2]\}$，是 H 的一個子群。

表 16.6

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

讓我們更仔細來看這個群 G。此處 $i^1=i$，$i^2=-1$，$i^3=-i$，及 $i^4=1$，所以 G 的每個元素是 i 的一個冪次方，且我們稱 i **生成** (generates) G。此被表為 $G=\langle i\rangle$。($G=\langle -i\rangle$ 亦為真，證明之。)

前一個例題的最後部份引我們至下面定義。

定義 16.6

群 G 被稱是**循環的** (cyclic) 若存在一個元素 $x \in G$ 滿足對每個 $a \in G$，$a=x^n$ 對某些 $n \in \mathbf{Z}$。

例題 16.13

a) 群 $H=(\mathbf{Z}_4, +)$ 是循環的。此處的運算是加法，所以我們有倍數代替冪次方。我們發現 [1] 和 [3] 兩者均生成 H。對 [3] 的情形，我們有 $1\cdot[3]=[3]$，$2\cdot[3](=[3]+[3])=[2]$，$3\cdot[3]=[1]$，及 $4\cdot[3]=[0]$。因此，$H=\langle[3]\rangle=\langle[1]\rangle$。

b) 考慮我們在例題 16.4 檢視過的乘法群 $U_9=\{1, 2, 4, 5, 7, 8\}$。此處我們發現 $2^1=2$，$2^2=4$，$2^3=8$，$2^4=7$，$2^5=5$，$2^6=1$，所以 U_9 是一個階數為 6 的循環群，且 $U_9=\langle 2\rangle$。$U_9=\langle 5\rangle$ 亦為真，因為 $5^1=5$，$5^2=7$，$5^3=8$，$5^4=4$，$5^5=2$，$5^6=1$。

循環群的概念引出一個相關概念。給一個群 G，若 $a \in G$，考慮集合 $S=\{a^k | k \in \mathbf{Z}\}$。由定理 16.2，得 S 是 G 的一個子群。這個子群被稱是**由 a 所生成的子群** (subgroup generated by a) 且被指定 $\langle a\rangle$。在例題 16.12，$\langle i\rangle=\langle -i\rangle=G$；而且，$\langle -1\rangle=\{-1, 1\}$ 及 $\langle 1\rangle=\{1\}$。對例題 16.13(a)，我們考慮倍數代替冪次方且發現 $H=\langle[1]\rangle=\langle[3]\rangle$，$\langle[2]\rangle=\{[0], [2]\}$，且 $\langle[0]\rangle=\{[0]\}$。當我們檢視該例題 (b) 中之群 U_9，我們看到 $U_9=\langle 2\rangle$(或 $\langle[2]\rangle$)=

$\langle 5\rangle$，$\langle 4\rangle = \{1, 4, 7\} = \langle 7\rangle$，$\langle 8\rangle = \{1, 8\}$，且 $\langle 1\rangle = \{1\}$。

定義 16.7

若 G 是一個群且 $a \in G$，則 a 的**階數** (order)，表為 $\mathbb{O}(a)$，是 $|\langle a\rangle|$。(若 $|\langle a\rangle|$ 是無限，我們稱 a 有無限階數。)

例題 16.12 裡，$\mathbb{O}(1) = 1$，$\mathbb{O}(-1) = 2$，而 i 和 $-i$ 均有階數 4。

讓我們再看一次當 $|\langle a\rangle|$ 是有限的情形時，階數的概念。當 $|\langle a\rangle| = 1$，則 $a = e$，因為 $a = a^1 \in \langle a\rangle$ 且 $e = a^0 \in \langle a\rangle$。若 $|\langle a\rangle|$ 是有限，但 $a \neq e$，則 $\langle a\rangle = \{a^m | m \in \mathbf{Z}\}$ 是有限，所以 $\{a, a^2, a^3, \cdots\} = \{a^m | m \in \mathbf{Z}^+\}$ 亦是有限。因此，存在 s，$t \in \mathbf{Z}^+$，其中 $1 \le s < t$ 且 $a^s = a^t$ ——因此得 $a^{t-s} = e$，其中 $t - s \in \mathbf{Z}^+$。因為 $e \in \{a^m | m \in \mathbf{Z}^+\}$，令 n 為最小的正整數滿足 $a^n = e$。我們要求 $\langle a\rangle = \{a, a^2, a^3, \cdots, a^{n-1}, a^n (= e)\}$。

首先我們觀察 $|\{a, a^2, a^3, \cdots, a^{n-1}, a^n (= e)\}| = n$。否則，我們有 $a^u = a^v$ 對正整數 u，v，其中 $1 \le u < v \le n$，且則 $a^{v-u} = e$，其中 $0 < v - u < n$。然而，此和 n 的最小數矛盾。所以現在我們知道 $|\langle a\rangle| \ge n$。但對每個 $k \in \mathbf{Z}$，由除法原理得 $k = qn + r$，其中 $0 \le r < n$，且所以 $a^k = a^{qn+r} = (a^n)^q (a^r) = (e^q)(a^r) = a^r \in \{a, a^2, a^3, \cdots, a^{n-1}, a^n (= e = a^0)\}$。因此，$\langle a\rangle = \{a, a^2, a^3, \cdots, a^{n-1}, a^n (= e)\}$ 且我們亦可定義 $\mathbb{O}(a)$ 為滿足 $a^n = e$ 的**最小正整數** (smallest positive integer) n。這個群元素的階數之替代定義證明下面定理的價值。

定理 16.6

令 $a \in G$ 且 $\mathbb{O}(a) = n$。若 $k \in \mathbf{Z}$ 且 $a^k = e$，則 $n | k$。

證明：由除法演算法 (再次)，我們有 $k = qn + r$，其中 $0 \le r < n$，且因而得 $e = a^k = a^{qn+r} = (a^n)^q (a^r) = (e^q)(a^r) = a^r$。若 $0 < r < n$，此和 $n = \mathbb{O}(a)$ 的定義矛盾。因此 $r = 0$ 且 $k = qn$。

我們現在檢視循環群的一些更進一步之結果。下一個例題幫我們刺激定理 16.7(b)。

例題 16.14

由例題 16.13(b)，得 $U_9 = \{1, 2, 4, 5, 7, 8\} = \langle 2\rangle$。我們使用這個事實，定義函數 $f: U_9 \to (\mathbf{Z}_6, +)$ 如下：

$$f(1) = [0] \qquad f(2) = [1] \qquad f(4) = [2]$$
$$f(5) = f(2^5) = [5] \qquad f(7) = f(2^4) = [4] \qquad f(8) = f(2^3) = [3]$$

所以，一般來講，對每個 $a \in U_9$，我們記 $a = 2^k$，且對某些 $0 \le k \le 5$，有

$f(a)=f(2^k)=[k]$。此函數 f 是一對一且映成，且我們發現，例如，$f(2\cdot 5)=f(1)=[0]=[1]+[5]=f(2)+f(5)$，且 $f(7\cdot 8)=f(2)=[1]=[4]+[3]=f(7)+f(8)$。

一般來講，對 a，b 屬於 U_9，我們可記 $a=2^m$ 且 $b=2^n$，其中 $0\le m\le 5$ 且 $0\le n\le 5$，且得

$$f(a\cdot b)=f(2^m\cdot 2^n)=f(2^{m+n})=[m+n]=[m]+[n]=f(a)+f(b)\,.$$

因此，函數 f 是一個同構函數且群 U_9 和 $(\mathbf{Z}_6,+)$ 是同構的。

[注意函數 f 是如何和兩個循環群的生成者連結。同時也注意函數 $g: U_9\to(\mathbf{Z}_6,+)$，其中

$g(1)=[0]$　　$g(5)=[1]$　　$g(7)=g(5^2)=[2]$
$g(8)=g(5^3)=[3]$　　$g(4)=g(5^4)=[4]$　　$g(2)=g(5^5)=[5]$

是介於這兩個循環群間的另一個同構函數。]

定理 16.7

令 G 是一個循環群。

a) 若 $|G|$ 是無限的，則 G 同構於 $(\mathbf{Z},+)$。
b) 若 $|G|=n$，其中 $n>1$，則 G 同構於 $(\mathbf{Z}_n,+)$。

證明：

a) 對 $G=\langle a\rangle=\{a^k|k\in\mathbf{Z}\}$，令 $f: G\to\mathbf{Z}$ 被定義為 $f(a^k)=k$。(我們會有 $a^k=a^t$ 且 $k\ne t$ 嗎？若有，f 將不是函數。) 對 a^m，$a^n\in G$，$f(a^m\cdot a^n)=f(a^{m+n})=m+n=f(a^m)+f(a^n)$，所以 f 是一個同態函數。我們留給讀者證明 f 是一對一且映成。
b) 若 $G=\langle a\rangle=\{a, a^2, \cdots, a^{n-1}, a^n=e\}$，則函數 $f: G\to\mathbf{Z}_n$ 被定義為 $f(a^k)=[k]$ 是一個同構函數。(證明這個)

例題 16.15

若 $G=\langle g\rangle$，則 G 是交換的，因為 $g^m\cdot g^n=g^{m+n}=g^{n+m}=g^n\cdot g^m$ 對所有 m，$n\in\mathbf{Z}$。然而，反之不成立。表 16.7 的群 H 是交換的，且 $\mathbb{O}(e)=1$，$\mathbb{O}(a)=\mathbb{O}(b)=\mathbb{O}(c)=2$。因為沒有 H 的元素的階數是 4，H 不可能是循環的。(群 H 是最小的非循環群且以 Klein Four 群命名。)

表 16.7

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

最後一個結果考慮循環群的子群結構。

定理 16.8 循環群的每個子群均是循環的。

證明：令 $G=\langle a\rangle$。若 H 是 G 的一個子群，H 的每個元素的型態為 a^k，對某些 $k\in\mathbf{Z}$。對 $H\neq\{e\}$，令 t 是最小的正整數滿足 $a^t\in H$。(我們是如何知道此一整數 t 存在呢？) 我們要求 $H=\langle a^t\rangle$。因為 $a^t\in H$，由子群 H 的封閉性，$\langle a^t\rangle\subseteq H$。對逆包含，令 $b\in H$，且 $b=a^s$，對某些 $s\in\mathbf{Z}$。由除法演算法，$s=qt+r$，其中 q，$r\in\mathbf{Z}$ 且 $0\le r<t$。因此，$a^s=a^{qt+r}$ 且所以 $a^r=a^{qt}a^s=(a^t)^{-q}b$。$H$ 是 G 的一個子群，所以 $a^t\in H\Rightarrow(a^t)^{-q}\in H$。則以 $(a^t)^{-q}$，$b\in H$，得 $a^r=(a^t)^{-q}b\in H$。但若 $a^r\in H$ 且 $r>0$，則我們矛盾了 t 的最小性。因此，$r=0$ 且 $b=a^{qt}=(a^t)^q\in\langle a^t\rangle$，所以 $H=\langle a^t\rangle$，一個循環群。

習題 16.2

1. 證明定理 16.5 的 (b) 和 (c)。
2. 令 $A=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$。
   a) 求 A^2，A^3，及 A^4。
   b) 證明 $\{A, A^2, A^3, A^4\}$ 在尋常矩陣乘法下是一個交換群。
   c) 證明 (b) 中之群同構於表 16.6 所示的群。
3. 若 $G=(\mathbf{Z}_6, +)$，$H=(\mathbf{Z}_3, +)$，且 $k=(\mathbf{Z}_2, +)$，找一個同構函數給群 $H\times K$ 和 G。
4. 令 $f: G\to H$ 是一個映成 H 的群同態函數。若 G 是交換的，證明 H 是交換的。
5. 令 $(\mathbf{Z}\times\mathbf{Z}, \oplus)$ 是交換群，其中 $(a, b)\oplus(c, d)=(a+c, b+d)$ ——此處 $a+c$ 及 $b+d$ 係以 $\mathbf{Z}$ 上尋常的加法計算——且令 $(G, +)$ 是一個相加的群。若 $f: \mathbf{Z}\times\mathbf{Z}\to G$ 是一個群同態，其中 $f(1, 3)=g_1$ 且 $f(3, 7)=g_2$，試以 g_1 和 g_2 來表示 $f(4, 6)$。
6. 令 $f: (\mathbf{Z}\times\mathbf{Z}, \oplus)\to(\mathbf{Z}, +)$ 為函數且被定義為 $f(x, y)=x-y$。[此處之 $(\mathbf{Z}\times\mathbf{Z}, \oplus)$ 和習題 5 的群相同，且 $(\mathbf{Z}, +)$ 是在尋常加法下的整數群。]
   a) 證明 f 是一個映成 $\mathbf{Z}$ 的同態函數。

b) 求所有的 $(a, b) \in \mathbf{Z}\times\mathbf{Z}$ 滿足 $f(a, b)=0$。

c) 求 $f^{-1}(7)$。

d) 若 $E=\{2n|n \in \mathbf{Z}\}$，求 $f^{-1}(E)$ ？

7. 分別對 (a) 等邊三角形；及 (b) 正方形的剛體運動群，求各個元素的階數。
8. 在 S_5 裡，找一個階數為 n 的元素，對所有 $2 \le n \le 5$。並決定這每一個元素所生成的 S_5 之(循環) 子群。
9. a) 求 $(\mathbf{Z}_{40}, +)$ 上所有階數為 10 的元素。

b) 令 $G=\langle a\rangle$ 是一個階數為 40 的循環群，G 的哪些元素的階數為 10？
10. a) 決定環 $(\mathbf{Z}_{14}, +, \cdot)$ 的可逆元素群 U_{14}。

b) 證明 U_{14} 是循環的並求它所有的生成者。
11. 證明 $(\mathbf{Z}_p^*, \cdot)$ 是循環的，對質數 5，7，和 11。
12. 對一個群 G，證明定義為 $f(a)=a^{-1}$ 的函數 $f: G \to G$ 是一個同構函數若且唯若 G 是交換的。
13. 若 $f: G \to H$，$g: H \to K$ 是同態函數，證明合成函數 $g \circ f: G \to K$，其中 $(g \circ f)(x)=g(f(x))$，是一個同態函數。
14. 對 $\omega=(1/\sqrt{2})(1+i)$，令 G 是乘法的群 $\{\omega^n|n \in \mathbf{Z}^+, 1 \le n \le 8\}$。

a) 證明 G 是循環的並找滿足 $\langle x\rangle=G$ 的每個元素 $x \in G$。

b) 證明 G 同構於群 $(\mathbf{Z}_8, +)$。
15. a) 找循環群 $(\mathbf{Z}_{12}, +)$，$(\mathbf{Z}_{16}, +)$，及 $(\mathbf{Z}_{24}, +)$ 的所有生成者。

b) 令 $G=\langle a\rangle$ 且 $\mathbb{O}(a)=n$。證明 a^k，$k \in \mathbf{Z}^+$，生成 G 若且唯若 k 和 n 互質。

c) 若 G 是一個階數為 n 的循環群，則它有多少個相異的生成者？
16. 令 $f: G \to H$ 是一個群同態函數。若 $a \in G$ 滿足 $\mathbb{O}(a)=n$ 及 $\mathbb{O}(f(a))=k$ (在 H 上)，證明 $k|n$。

16.3　傍集及 Lagrange 定理

在上兩節裡，對所有的有限群 G 及 G 的子群 H，我們有 $|H|$ 整除 $|G|$。本節我們將看到這不僅是機運，而是一般上均為真。欲證明這個我們需一個新概念。

定義 16.8

若 H 是 G 的一個子群，則對每個 $a \in G$，集合 $aH=\{ah|h \in H\}$ 被稱是 H 在 G 上的一個**左傍集** (left coset)。集合 $Ha=\{ha|h \in H\}$ 是 H 在 G 上的一個**右傍集** (right coset)。

若 G 上的運算是加法，我們以 $a+H$ 取代 aH，其中 $a+H=\{a+h|h \in H\}$。

當**傍集** (coset) 這個名詞被使用於本章時，它將被述為左傍集。對交換群，沒有需要來分辨左右傍集。然而，在下一個例題文末，我們將看到交換群不是這個樣子。

例題 16.16

若 G 是例題 16.7 的群且 $H=\{\pi_0, \pi_1, \pi_2\}$，則傍集 $r_1H=\{r_1\pi_0, r_1\pi_1, r_1\pi_2\}=\{r_1, r_2, r_3\}$。同樣的，我們有 $r_2H=r_3H=\{r_1, r_2, r_3\}$，而 $\pi_0H=\pi_1H=\pi_2H=H$。

我們看到 $|\alpha H|=|H|$ 對每個 $\alpha \in G$ 且 $G=H \cup r_1H$ 是 G 的一個分割。

對子群 $K=\{\pi_0, r_1\}$，我們發現 $r_2K=\{r_2, \pi_2\}$ 且 $r_3K=\{r_3, \pi_1\}$。再出現 G 的一個分割：$G=K \cup r_2K \cup r_3K$。(注意：$Kr_2=\{\pi_0r_2, r_1r_2\}=\{r_2, \pi_1\} \neq r_2K$。)

例題 16.17

對 $G=(\mathbf{Z}_{12}, +)$ 及 $H=\{[0], [4], [8]\}$，我們發現

$$[0]+H=\{[0], [4], [8]\}=[4]+H=[8]+H=H$$
$$[1]+H=\{[1], [5], [9]\}=[5]+H=[9]+H$$
$$[2]+H=\{[2], [6], [10]\}=[6]+H=[10]+H$$
$$[3]+H=\{[3], [7], [11]\}=[7]+H=[11]+H$$

且 $H \cup ([1]+H) \cup ([2]+H) \cup ([3]+H)$ 是 G 的一個分割。

這些例題提供我們下面結果。

引理 16.1

若 H 是有限群 G 的一個子群，則對所有 a，$b \in G$，(a) $|aH|=|H|$；且 (b) 不是 $aH=bH$ 就是 $aH \cap bH=\emptyset$。

證明：

a) 因為 $aH=\{ah|h \in H\}$，得 $|aH| \leq |H|$。若 $|aH|<|H|$，我們有 $ah_i=ah_j$，其中 h_i，h_j 為 H 的相異元素。由 G 的左邊-消去律，得 $h_i=h_j$ 的矛盾，所以 $|aH|=|H|$。

b) 若 $aH \cap bH \neq \emptyset$，令 $c=ah_1=bh_2$，對某些 h_1，$h_2 \in H$。若 $x \in aH$，則 $x=ah$，對某些 $h \in H$，且所以 $x=(bh_2h_1^{-1})h=b(h_2h_1^{-1}h) \in bH$ 且 $aH \subseteq bH$。同理 $y \in bH \Rightarrow y=bh_3$，對某些 $h_3 \in H \Rightarrow y=(ah_1h_2^{-1})h_3=a(h_1h_2^{-1}h_3) \in aH$，所以 $bH \subseteq aH$。因此 aH 和 bH 不是互斥就相同。

我們觀察到若 $g \in G$，則 $g \in gH$，因為 $e \in H$。而且，由引理 16.1

(b)，G 可被分割成互斥的傍集。

此刻我們已準備好來證明本節的主要結果。

定理 16.9

Lagrange 定理 (Lagrange Theorem)。若 G 是一個階數為 n 的有限群，且 H 是一個階數為 m 的子群，則 m 整除 n。

證明：若 $H=G$，結果成立。否則 $m<n$ 且存在一個元素 $a \in G-H$。因為 $a \notin H$，得 $aH \neq H$，所以 $aH \cap H = \emptyset$。若 $G=aH \cup H$，則 $|G|=|aH|+|H| = 2|H|$ 且定理成立。若否，存在一個元素 $b \in G-(H \cup aH)$，且 $bH \cap H = \emptyset = bH \cap aH$ 及 $|bH|=|H|$。若 $G=bH \cup aH \cup H$，我們有 $|G|=3|H|$。否則，我們回到一個元素 $c \in G$ 滿足 $c \notin bH \cup aH \cup H$。群 G 是有限的，所以這個過程將終止且我們發現 $G=a_1H \cup a_2H \cup \cdots \cup a_kH$。因此，$|G| = k|H|$ 且 m 整除 n。

另一個證明這個定理的方法被給在本節的習題 12。

我們以兩個系理的敘述作為結束。它們的證明被要求在本節習題裡。

系理 16.1

若 G 是一個有限群且 $a \in G$，則 $\mathbb{O}(a)$ 整除 $|G|$。

系理 16.2

每個質階數的群是循環的。

習題 16.3

1. 令 $G=S_4$。(a) 對 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$，求子群 $H=\langle\alpha\rangle$。 (b) 決定 H 在 G 上的左傍集。
2. 若 α 被取代為 $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$，回答習題 1。
3. 若 $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$，則 $\langle\gamma\rangle$ 有多少個傍集？
4. 對 $G=(\mathbf{Z}_{24}, +)$，求由子群 $H=\langle[3]\rangle$ 所決定的所有傍集。對子群 $K=\langle[4]\rangle$ 做相同的事。
5. 令 G 是一個含子群 H 和 K 的群。若 $|G|=660$，$|K|=66$，且 $K \subset H \subset G$，則 $|H|$ 的所有可能值為何？
6. 令 R 是一個具單位元素 u 的環。證明 R 的所有可逆元素在環的乘法下形成一個群。
7. 令 $G=S_4$，含四個符號的對稱群，且令 H 是 G 的子集合，其中

$$H = \left\{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\right\}.$$

a) 建構一個表來證明 H 是 G 的一個交換群。

b) G 上有多少個 H 的左傍集？

c) 考慮群 $(\mathbf{Z}_2 \times \mathbf{Z}_2, \oplus)$，其中 $(a, b) \oplus (c, d) = (a+c, b+d)$ ——和 $a+c$，$b+d$ 係以加法模 2 來算。證明 H 同構於這個群。

8. 若 G 是一個階數為 n 的群且 $a \in G$，證明 $a^n = e$。
9. 令 p 為一個質數。(a) 若 G 有階數 $2p$，證明 G 的每個真子群是循環的。(b) 若 G 有階數 p^2，證明 G 有一個階數為 p 的子群。
10. 證明系理 16.1 及 16.2。
11. 令 H 和 K 是群 G 的子群，其中 e 是 G 的單位元素。

a) 證明若 $|H| = 10$ 且 $|K| = 21$，則 $H \cap K = \{e\}$。

b) 若 $|H| = m$ 且 $|K| = n$ 滿足 $\gcd(m, n) = 1$，證明 $H \cap K = \{e\}$。

12. 下面提供另一法來建立 Lagrange 定理。令 G 是一個階數為 n 的群，且令 H 是一個階數為 m 的 G 之子群。

a) 定義 G 上的關係 $\mathcal{R}$ 如下：若 $a, b \in G$，則 $a \mathcal{R} b$ 若 $a^{-1}b \in H$。證明 $\mathcal{R}$ 是 G 上的一個等價關係。

b) 對 $a, b \in G$，證明 $a \mathcal{R} b$ 若且唯若 $aH = bH$。

c) 若 $a \in G$，證明 $[a]$，a 在 R 之下的等價關係，滿足 $[a] = aH$。

d) 對每個 $a \in G$，證明 $|aH| = |H|$。

e) 現在建立 Lagrange 定理的結論，即 $|H|$ 整除 $|G|$。

13. a) *Fermat* 定理。若 p 是質數，證明 $a^p \equiv a \pmod p$ 對每個 $a \in \mathbf{Z}$。[這和 14.3 節習題 22(a) 有何關係？]

b) *Euler* 定理。對每個 $n \in \mathbf{Z}^+$，$n > 1$，且每個 $a \in \mathbf{Z}$，證明若 $\gcd(a, n) = 1$，則 $a^{\phi(n)} \equiv 1 \pmod n$。

c) (a) 和 (b) 中之兩定理有何關係？

d) 這兩個定理和習題 6 及 8 有何關聯？

16.4 RSA 密碼系統 (可選擇的)

本節提供我們一個機會，使用一些我們在 14.3 節及 16.3 節所見到的理論概念於一個較現代的應用裡。

在 14.3 節例題 14.15，我們介紹兩個隱遁的鍵值密碼系統：即密碼推移及仿射密碼。對一個含 m 個字元的字母集，譯成密碼函數 $E: \mathbf{Z}_m \to \mathbf{Z}_m$，其對密碼-推移密碼系統，被給為 $E(\theta) = (\theta + \kappa) \bmod m$，其中 $\theta, \kappa \in \mathbf{Z}_m$，對 κ ($\neq 0$) 固定。(使用 $k = 0$ 將不改變訊息裡的任何一個字元。) 因此，有 $m-1$ 個可能來檢視以便發現鍵值 κ。更而，一旦我們知道 κ 值，我們亦知破解密語函數 $D: \mathbf{Z}_m \to \mathbf{Z}_m$，其中 $D(\theta) = (\theta - \kappa) \bmod m$。而在仿射密碼密碼系統裡 (亦以一個含 m 個字元的字母集)，譯成密碼函數 $E: \mathbf{Z}_m$

$\rightarrow \mathbf{Z}_m$ 被給為 $E(\theta) = (\alpha\theta + \kappa)$ **mod** m，其中 θ，α，$\kappa \in \mathbf{Z}_m$，對固定的 α，κ，且 α 在 $\mathbf{Z}_m$ 上可逆[或等價地，$\gcd(\alpha, m) = 1$]。這裡破解密語函數 $D : \mathbf{Z}_m \rightarrow \mathbf{Z}_m$ 被給為 $D(\theta) = [\alpha^{-1}(\theta - \kappa)]$ **mod** m。在沒有鍵值 (α, κ) 的先前知識下，現在我們將必須檢查 $m\phi(m)$ 個可能來發現適合的 α 及 κ 值給這個隱遁鍵值密碼系統。

上面兩個密碼系統之任何一個的安全性依賴僅有訊息寄發者及收件者知道的鍵值 (即 κ 值或 (α, κ) 值]。

RSA 密碼系統是一個**公開-鍵值** (public-key) 的密碼系統例子。這個密碼系統由的 Ronald Rivest (1948-)，Adi Shamir (1952-)，及 Leonard Adleman (1945-) 所發展的。(取這三位每個人姓氏的第一個字母而得形容詞 RSA。)

我們將描述這個密碼系統如何運作，並提供一個例題給譯成密碼及破解密語。在如此進行時，我們將發現我們使用 14.3 節及 16.3 節的一些結果。

例題 16.18

如同在兩個隱遁鍵值密碼系統，我們再次有一個含 m 個字元的字母集。我們以兩個相異質數 p，q 開始。實際上，它們應是大的質數——每一個有 100 或更多位數。(然而，在我們的例題裡，我們將使用較小的質數。) 在選了質數 p，q 之後，我們接著考慮整數 $n = pq$ 及 $r = (p-1)\cdot(q-1) = \phi(p)\phi(q) = \phi(pq) = \phi(n)$，且此刻，我們在 $\mathbf{Z}_r = (\mathbf{Z}_{\phi(n)})$ 上選一個可逆元素 e。

[此處，若元素 e 隨機選出，則唯一我們無法得到可逆元素的是當所選的元素是 p 的一個倍數 (有 q 個可能) 或 q 的一個倍數 (有 p 個可能) 時。在這個我們所說明的 $p+q$ 個元素的總數中，我們計數 pq 兩次，所以僅有 $p+q-1$ 個可能會失敗。因此，失敗的機率是 $(p+q-1)/(pq) = (1/q) + (1/p) - (1/(pq))$，是一個非常小的數若 p 和 q 有 100 或更多的位數。]

例如，考慮 $p = 61$，$q = 127$，則 $n = (61)(127) = 7747$ 且 $r = \phi(61)\cdot\phi(127) = (60)(126) = 7560$。現在假設我們選 e 為 17。

考慮下面訊息，我們想將它譯成密碼。

INVEST IN BONDS

利用例題 14.15(b) 所指派的明語，在這裡我們將字母 "I" 改為 08 (不僅是 8)。接著我們將 "N" 改為 13。此提供我們第一個四個數字的區組——即 0813 ——給前兩個字母 "IN"。完整訊息的指派如下 [其中我們已將字母 "X" 附加在右端，以使最後的區組有兩個字母 (或四個數字)]：

I	N	V	E	S	T	I	N	B	O	N	D	S	X
08	13	21	04	18	19	08	13	01	14	13	03	18	23

我們現在利用譯成密碼數 E 將每個四個數字的區組 B 譯成密碼，其中 $E(B)=B^e \bmod n$。(這個模指數可利用例題 14.16 的方法有效的算出。) 所以此處 E 的定義域是 $\mathbf{Z}_{26}$ 和本身串聯，且我們發現

$0813^{17} \bmod 7747 = 2169$　　$2104^{17} \bmod 7747 = 0628$　　$1819^{17} \bmod 7747 = 5540$
$0813^{17} \bmod 7747 = 2169$　　$0114^{17} \bmod 7747 = 6560$　　$1303^{17} \bmod 7747 = 6401$
$1823^{17} \bmod 7747 = 4829.$

因此，譯成密碼指派 (給所給的明語訊息) 的接受者接受密語

2169　0628　5540　2169　6560　6401　4829.

現在的問題是：“接受者如何破解所接到的密語呢？”

因為 e 是 $\mathbf{Z}_r$ ($=\mathbf{Z}_{\phi(n)}$) 上的一個可逆元素，我們可使用歐幾里得演算法 (如例題 14.13) 來計算 $e^{-1}=d$。接著我們定義破解密語函數 D，其中 $D(C)=C^d \bmod n$，對一個四個數字的區組 C。由於 $e^{-1}=d$，得 $ed \equiv 1 \bmod \phi(n)$ ——亦即 $ed \bmod \phi(n)=1$。因此，$ed=k\phi(n)+1$，對某些 $k \in \mathbf{Z}$。現在回憶早先所給的機率理論，由 $\mathbf{Z}_n$ 隨機選取的元素 e 是可逆的 (或是 $\mathbf{Z}_n$ 上的可逆元素)。對任意四個數字的區組 B，我們考慮 B 為 $\mathbf{Z}_n$ 上的一元素——事實上，我們考慮 B 為 $\mathbf{Z}_n$ 上的一個可逆元素。因為環 $(\mathbf{Z}_n, +, \cdot)$ 上的所有可逆元素在乘法之下形成一個階數為 $\phi(n)$ 的群，由 16.3 節習題 8 的結果，得 $B^{ed}=B^{k\phi(n)+1}=(B^{\phi(n)})^k B^1 \equiv B \pmod n$，或 $B^{ed} \bmod n = B$。[這亦是 Euler 定理的一個結果，如 16.3 節習題 13(b) 所敘述的。]

應用本例前段的結果，我們有 $p=61$，$q=127$，$n=pq=7747$，$r=\phi(n)=(p-1)(q-1)=(60)(126)=7560$，及 $e=17$。由歐幾里得演算法，得 $d=e^{-1}=3113$。現在我們發現，例如，$2169^{3113} \bmod 7747 = 0813$ 且 $0628^{3113} \bmod 7747 = 2104$。繼續下去，接受者可決定數值指派給原先的明語及後續的明語。

現在是什麼使 RSA 密碼系統比我們所學的隱遁-鍵值密碼系統更為安全呢？首先，我們應敘述 RSA 密碼系統不是一個隱遁-鍵值密碼系統。此系統是一個公開-鍵值的密碼系統之一例子，其中鍵值 (n, e) 是公開的。所以看起來，欲破解已譯成的密碼指派，所需做的是決定 $d=e^{-1}$ 於 $\mathbf{Z}_r$ ($=\mathbf{Z}_{\phi(n)}$) 上。現在是時刻來瞭解，知道 n 值我們是無法立刻知道 r 值的。為

要能決定 $r=(p-1)(q-1)$，我們需要知道 p，q 值，即 n 的質因數。這就是使這個系統比其它我們提過的密碼系統更更安全的原因。欲決定質數 p，q，當它們是 100 或更長數字時，不是一個可行的問題。然而，當電腦的功能繼續改進時，欲保有 RSA 密碼系統的安全，吾人可能需要使用更多更多數字的質數來重新定義鍵值。

在結束時，我們證明分解模 n 的問題和決定 $r=(p-1)(q-1)$ 的問題是如何相關的。我們以觀察

$$p+q=pq-(p-1)(q-1)+1=n-\phi(n)+1=n-r+1.$$

開始，而

$$\begin{aligned} p-q &= \sqrt{(p-q)^2}=\sqrt{(p-q)^2+4pq-4pq}=\sqrt{(p+q)^2-4pq} \\ &= \sqrt{(p+q)^2-4n}=\sqrt{(n-r+1)^2-4n}. \end{aligned}$$

則由這兩方程，我們學到

$$p=(1/2)[(p+q)+(p-q)]=(1/2)[(n-r+1)+\sqrt{(n-r+1)^2-4n}]$$

且

$$q=(1/2)[(p+q)-(p-q)]=(1/2)[(n-r+1)-\sqrt{(n-r+1)^2-4n}].$$

因此，當我們知道 n 和 r 時，我們就可決定質數 p，q 滿足 $n=pq$。

習題 16.4

強烈推荐前面四個習題使用電腦代數系統。

1. 決定明語 INVEST IN STOCKS 的密語，以 $e=7$ 及 $n=2573$ 使用 RSA 編譯密碼。
2. 決定明語 ORDER A PIZZA，以 $e=5$ 及 $n=1459$ 使用 RSA 編譯密碼。
3. 決定 RAS 密語 1418 1436 2370 1102 1805 0250 的明語，若 $e=11$ 及 $n=2501$。
4. 決定 RAS 密語 0986 3029 1134 1105 1232 2281 2967 0272 1818 2398 1153 的明語，若 $e=17$ 及 $n=3053$。
5. 求質數 p，q 若 $n=pq=121{,}361$ 且 $\phi(n)=120{,}432$。
6. 求質數 p，q 若 $n=pq=5{,}446{,}367$ 且 $\phi(n)=5{,}441{,}640$。

16.5 編碼理論的要素

在本節及下面四節，我們將介紹一個所謂的**代數編碼理論** (algebraic coding theory) 的應用數學領域。這個理論受到 Glaude Shannon (1948) 的基本論文及 Marcel Golay (1949) 和 Richard Hamming (1950) 之結果的鼓舞。從那刻起，它成為一個被大感興趣的領域，其中代數結構、機率，及組合學等均扮演一個角色。

我們的教材將擁有一個介紹層次，當我們尋找模擬以符號 0 和 1 之字串所表示的資訊之傳送時。

在數位傳達時，當資訊以由幾個 0 和幾個 1 的形式來傳遞時，某種問題產生。由於頻道的吵雜結果，當某一個訊號被傳遞時，可能會接受到一個不同的訊號，導致接受者做錯誤的決定。因此，我們想發展一些方法來幫助我們偵測，也許甚至修正傳送錯誤。然而，我們僅能改進修正傳送的機會，但不保證。

我們的模型使用一個**二元對稱頻道** (binary symmertic channel)，如圖 16.2 所示。形容詞二元出現係因為一個個別訊號係以位元 0 或 1 中之一表示。當一個傳導體以此一個頻道傳送訊號 0 或 1 時，每一個訊號結合一個 (常數) 機率 p 給不正確的傳送。當對兩個訊號的機率 p 相同時，稱這個頻道是**對稱的** (symmetric)。例如，我們有送出 0 且接收到 1 的機率為 p，則送出訊號 0 且正確接到 0 的機率是 $1-p$。所有的機率被展示於圖 16.2。

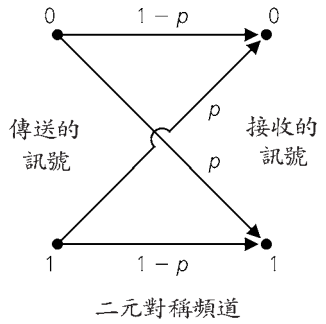


圖 16.2

例題 16.19

考慮串 $c=10110$。我們將 c 視為群 $\mathbf{Z}_2^5$ 的一個元素，其中 $\mathbf{Z}_2^5$ 是五個 $(\mathbf{Z}_2, +)$ 的直線。欲簡化記號，我們記 10110 代替 (1, 0, 1, 1, 0)。當經過二元對稱頻道送出 c 的每個位元 (個別訊號) 時，我們假設不正確傳送的機率是 $p=0.05$，使得沒有錯誤傳送 c 的機率是 $(0.95)^5 \doteq 0.77$。

這裡及整個編碼理論，我們假設每個訊號的傳送和前面訊號的傳送方法無關。因此，所有這些**獨立** (independent) 事件 (以它們的規定順位) 發生的機率是它們個別機率的乘積。

接收 5-位元訊息的派對接收串 $r=00110$ 的機率是多少？亦即，錯誤在第一個位置的原始訊息。第一個位元錯誤傳送的機率是 0.05，由於獨立事件的假設，所以傳送 $c=10110$ 且接收 $r=00110$ 的機率是 $(0.05)(0.95)^4 \doteq 0.041$。以 $e=10000$，我們可寫 $c+e=r$，且將 r 解讀為原始訊息 c 及特別**錯誤型** (error pattern) $e=10000$ 之和的結果。因為 $c, r, e \in \mathbf{Z}_2^5$ 且 $-1=1$ 在 $\mathbf{Z}_2$ 上，我們亦有 $c+r=e$ 及 $r+e=c$。

在傳送 $c=10110$ 時，接收 $r=00100$ 的機率是

$$(0.05)(0.95)^2(0.05)(0.95) \doteq 0.002,$$

所以這個乘法錯誤是不太可能發生。

最後，若我們傳送 $c=10110$，則 r 和 c 恰有兩個位置相異的機率是多少？欲回答這個，我們將每個由兩個 1 及三個 0 所組成的錯誤型之機率加起來。每個錯誤型的機率是 0.002。共有 $\binom{5}{2}$ 個這樣的錯誤型，所以傳送時兩個錯誤的機率是

$$\binom{5}{2}(0.05)^2(0.95)^3 \doteq 0.021.$$

這些結果引我們至下面定理。

定理 16.10

令 $c \in \mathbf{Z}_2^n$。對經過一個二元對稱頻道的 c 之傳送，其中錯誤傳送的機率為 p。

a) 接收 $r=c+e$ 的機率是 $p^k(1-p)^{n-k}$，其中 e 是一個由 k 個 1 及 $(n-k)$ 個 0 所組成的特別錯誤型。

b) 在傳送中 (恰有) k 個錯誤的機率是

$$\binom{n}{k}p^k(1-p)^{n-k}.^{\dagger}$$

在例題 16.19 裡，$c=10110$ 的傳送中，至多一個錯誤的機率是 $(0.95)^5 + \binom{5}{1}(0.05)(0.95)^4 \doteq 0.977$。因此，在傳送中，多個錯誤的機會在本章的整個討論裡將不考慮。此一假設是有效的當 p 是很小時。事實上，一個

† 這是發展於 (可選擇的) 3.5 節及3.7 節之二項式機率分配。

二元對稱頻道被認為是“好的”當 $p<10^{-5}$ 時。然而，不管我們有什麼約定，我們總是希望 $p<1/2$。

欲改進二元對稱頻道傳送的正確性，某種型態的編碼格式可被使用，其中額外的位元被供給。

對 m，$n\in\mathbf{Z}^+$，令 $n>m$。考慮 $\emptyset\neq W\subseteq\mathbf{Z}_2^m$。集合 W 由訊息 (messages) 所組成且待被傳送。我們附加 $n-m$ 個額外位元至每個 $w\in W$ 來形成**碼字** (code word) c，其中 $c\in\mathbf{Z}_2^n$。這個過程叫做**編碼** (encoding) 且以函數 $E: W\to\mathbf{Z}_2^n$ 來表示。則 $E(w)=c$ 且 $E(W)=C\subseteq\mathbf{Z}_2^n$。因為函數 E 簡單的附加額外的位元至所有 (相異的) 訊息，編碼過程是一對一。在傳送方面，c 被接收為 $T(c)$，其中 $T(c)\in\mathbf{Z}_2^n$。不幸地，T 不是一個函數，因為 $T(c)$ 在不同的傳送時間可能不同 (因為頻道中的吵雜度隨時間而改變)。 (參見圖 16.3)

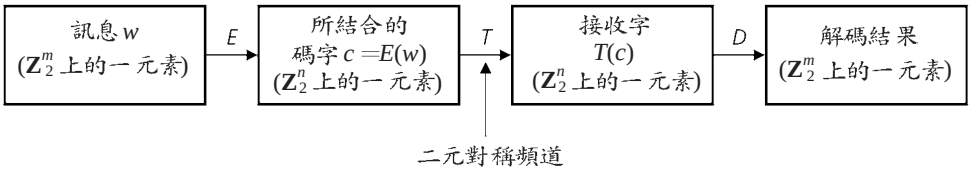


圖 16.3

一旦接收到 $T(c)$，我們想應用一個解碼函數 $D:\mathbf{Z}_2^n\to\mathbf{Z}_2^m$ 來移走額外的位元，且我們希望得到原先的訊息 w。理想的 $D\circ T\circ E$ 應為 W 上的單位函數，且 $D: C\to W$。因為這個不可能預期，我們找尋函數 E 和 D 使得有一個高機率的正確解碼所接收的字 $T(c)$ 並取回原先的訊息 w。此外，在得到碼字 $c=E(w)$ 時，我們想令比率 m/n 為儘可能的大，使得多餘的位元數不被附加至 w。比率 m/n 測量我們的格式之**效率** (efficiency) 且被稱為碼的**速率** (rate)。最後，函數 E 和 D 應多於理論結果；它們必為實際的可被電子執行。

在此一個格式裡，函數 E 和 D 分別被稱是一個 (n, m) 區組碼的**編碼** (encoding) 及**解碼** (decoding) 函數。

我們說明這些概念於下面兩個例題裡。

例題 16.20

考慮 $(m+1, m)$ 區組碼，其中 $m=8$。令 $W=\mathbf{Z}_2^8$。對每個 $w=w_1w_2\cdots w_8\in W$，定義 $E:\mathbf{Z}_2^8\to\mathbf{Z}_2^9$ 為 $E(w)=w_1w_2\cdots w_8w_9$，其中 $w_9=\sum_{i=1}^{8}w_i$，具模 2 的加法。例如 $E(11001101)=110011011$，且 $E(00110011)=001100110$。

對所有 $w\in\mathbf{Z}_2^8$，$E(w)$ 有偶數個 1。所以，對 $w=11010110$ 及 $E(w)=$

110101101，若我們接收 $T(c)=T(E(w))$ 為 100101101，由 $T(c)$ 中的奇數個 1，我們知道在傳送中有一個錯誤發生。因此，我們能偵察出傳送中的單一錯誤。但我們似乎沒有方法來修正此類錯誤。

寄發碼字 110101101 且在傳送中至多一個錯誤的機率是

$$\underbrace{(1-p)^9}_{\text{所有 9 個位元正確傳送}}+\underbrace{\binom{9}{1}p(1-p)^8}_{\text{一個位元於傳送中改變且一個錯誤被偵測出來}}.$$

對 $p=0.001$，此得 $(0.999)^9+\binom{9}{1}(0.001)(0.999)^8\doteq 0.99996417$。

若我們偵測到一個錯誤且我們可以更新一個訊號回到傳送器，重做碼字的傳送，且繼續這個方法，直到接收的字有偶數個 1，則寄發碼字 110101101 且接收正確傳送的機率大約是 0.99996393。†

若傳送中有正偶數個錯誤發生，$T(c)$ 不幸地被接受為正確的碼且我們解讀其前八個分子為原始訊息。這個格式被稱是 $(m+1, m)$ **奇偶性-校驗碼** (parity-check code) 且僅適合於當多重錯誤不可能發生時。

若我們經由頻道寄發訊息 11010110，我們有 $(0.999)^8=0.99202794$ 的正確傳送機率。利用奇偶性-校驗碼，我們得到正確訊息的機會增加至大約 0.99996393。然而一個額外的訊號被寄發 (且或許額外的傳送是需要的) 且碼的速率由 1 遞減至 8/9。

但假設我們不是寄發 8 個位元而是 160 個位元，逐次的以長度為 8 的串。沒有任何碼格式而接收到正確訊息的機會將是為 $(0.999)^{160}\doteq 0.85207557$。以奇偶性-校驗法寄發 180 個位元，正確傳送的機會將增加至 $(0.999964)^{20}\doteq 0.99928025$。

例題 16.21

$(3m, m)$ **三重重複碼** (triple repetition code) 是一個我們可偵測並修正傳送中單一錯誤的碼。以 $m=8$ 及 $W=\mathbf{Z}_2^8$，我們定義 $E:\mathbf{Z}_2^8\to\mathbf{Z}_2^{24}$ 為 $E(w_1w_2\cdots w_7w_8)=w_1w_2\cdots w_8w_1w_2\cdots w_8w_1w_2\cdots w_8$。

因此，若 $w=10110111$，則 $c=E(w)=101101111011011110110111$。

解碼函數 $D:\mathbf{Z}_2^{24}\to\mathbf{Z}_2^8$ 被以主要規則來執行。例如，若 $T(c)=$

---

† 對 $p=0.001$，在碼字 110101101 的傳送中奇數個錯誤發生的機率是

$$p_{\text{odd}}=\binom{9}{1}(0.999)^8(0.001)+\binom{9}{3}(0.999)^6(0.001)^3+\binom{9}{5}(0.999)^4(0.001)^5+\binom{9}{7}(0.999)^2(0.001)^7+\binom{9}{9}(0.001)^9$$
$$\doteq 0.008928251+0.000000083+0.000000000+0.000000000+0.000000000=0.008928334.$$

以 $q=$110101101的正確傳送機率 $=(0.999)^9$，這個碼字被傳送且在這些(再傳送) 的條件下被正確接收的機率是

$$q+p_{\text{odd}}\cdot q+(p_{\text{odd}})^2q+(p_{\text{odd}})^3q+\cdots=q/(1-p_{\text{odd}})\doteq 0.99996393 \text{ 至小數點第八位}$$

101001110011011110110110，則我們有三個錯誤發生於位置 4，9 及 24。我們以檢視第一、第九，及第十七位置看看哪一個訊號出現較多次，來解碼 $T(c)$。此時是 1 (其發生兩次)，所以我們將解碼訊息中的第一個元素解碼為 1。以第二、第十，及第十八位置的元素繼續，得解碼訊息的第二個元素為 0 (其均發生三次)。如此繼續，我們取回正確訊息 10110111。

雖然此處我們有多於一個的傳送錯誤，但所有的是良好的，除非兩個 (或更多個) 錯誤發生，其中第二個錯誤是第一個之後的八格或 16 格——亦即，若兩個 (或更多個) 不正確傳送發生給原始訊息的相同位元。

這個格式如何與其它我們已有的方法做比較呢？以 $p=0.001$，正確解碼一個單一位元的機率是 $(0.999)^3+\binom{3}{1}(0.001)(0.999)^2 \doteq 0.99999700$。所以接收並正確解碼八位元訊息的機率是 $(0.99999700)^8=0.99997600$，僅稍為比由奇偶性-校驗法所得的結果好一點 (其中我們可能必須重傳送，因此增加整個傳送時間)。這裡我們傳送 24 個訊號給這個訊息，所以我們的速率是 1/3。因為這個增加正確性及偵測修正單一錯誤的能力 (我們在前面任何格式中無法辦到)，我們願付所增加的傳送時間。但我們不願浪費重傳送的時間。

習題 16.5

1. 令 C 為碼字集合，其中 $C \subseteq \mathbf{Z}_2^7$。在下面各小題中，給了 e (錯誤型)，r (接收的字) 及 c (碼字) 中的兩個，其中 $r=c+e$。試求第三項。
   a) $c=1010110$，$r=1011111$
   b) $c=1010110$，$e=0101101$
   c) $e=0101111$，$r=0000111$
2. 一個二元對稱頻道的不正確傳送機率為 $p=0.05$。若碼字 $c=011011101$ 被傳送，則 (a) 我們接收 $r=011111101$ 的機率為何？(b) 我們接收 $r=111011100$ 的機率為何？(c) 一個單一錯誤發生的機率為何？(d) 一個兩個錯誤發生的機率為何？(e) 三個錯誤發生的機率為何？(f) 三個錯誤發生，其中無兩個連續發生的機率為何？
3. 令 $E:\mathbf{Z}_2^3 \to \mathbf{Z}_2^9$ 為給 (9, 3) 三重重複碼的編碼函數。
   a) 若 $D:\mathbf{Z}_2^9 \to \mathbf{Z}_2^3$ 是對應的解碼函數，應用 D 來解碼所接收的字 (i) 111101100; (ii) 000100011; (iii) 010011111。
   b) 找三個不同的接收字 r 滿足 $D(r)=000$。
   c) 對每個 $w \in \mathbf{Z}_2^3$，$|D^{-1}(w)|$ 值為何？
4. $(5m, m)$ 五次重複碼有編碼函數 $E:\mathbf{Z}_2^m \to \mathbf{Z}_2^{5m}$，其中 $E(w)=wwwww$。以主要規劃來執行解碼 $D:\mathbf{Z}_2^{5m} \to \mathbf{Z}_2^m$。(這裡我們能於傳送中修正單一及雙重錯誤。)
   a) 以 $p=0.05$，傳送及正確解碼訊號 0 的機率為何？

b) 以訊息 110 代替訊號 0，回答 (a)。

c) 對 $m=2$，解碼接收字 $r=01110$ 01001。

d) 若 $m=2$，找三個接收字 r 滿足 $D(r)=00$。

e) 對 $m=2$ 且 $D:\mathbf{Z}_2^{10}\to\mathbf{Z}_2^2$，對每個 $w\in\mathbf{Z}_2^2$，$|D^{-1}(w)|$ 值為何？

16.6　Hamming 度量

本節我們將發展一般原理來討論一個編碼格式的錯誤-偵測及錯誤-修正的可能性。這些概念係由 Richard Wesley Hamming (1915-1998) 所發展的。

我們以考慮一個碼 $C\subseteq\mathbf{Z}_2^4$ 開始，其中 $c_1=0111$，$c_2=1111\in C$。現在傳送者及接收者均認識 C 的所有元素。所以，若傳送者送出 c_1，但接收者接收的碼字 $T(c_1)$ 為 1111，則他或她感覺到被傳送的是 c_2 且做一個 c_2 蘊涵的決策 (錯誤的決策)。因此，雖然僅有一個傳送錯誤發生，但結果可能是不愉快的。為何這樣呢？不幸地，我們有兩個幾乎相同的碼字。它們是頗互相接近的，因為它們僅差異一個分量。

我們更清楚的描述這個接近觀念如下。

定義 16.9

對每個元素 $x=x_1x_2\cdots x_n\in\mathbf{Z}_2^n$，其中 $n\in\mathbf{Z}^+$，x 的**權數** (weight)，表為 $\text{wt}(x)$，是 x 的分量 x_i 的個數，其中 $1\le i\le n$ 且 $x_i=1$。若 $y\in\mathbf{Z}_2^n$，x 和 y 間的**距離** (distance)，表為 $d(x,y)$，是 $x_i\neq y_i$ 的分量個數，對 $1\le i\le n$。

例題 16.22

對 $n=5$，令 $x=01001$ 且 $y=11101$，則 $\text{wt}(x)=2$，$\text{wt}(y)=4$，且 $d(x,y)=2$。在加法上，$x+y=10100$，所以 $\text{wt}(x+y)=2$。有機會剛好 $d(x,y)=\text{wt}(x,y)$ 嗎？對每個 $1\le i\le 5$，x_i+y_i 貢獻一個 1 的計數給 $\text{wt}(x,y)\Leftrightarrow x_i\neq y_i\Leftrightarrow x_i$，$y_i$ 貢獻一個 1 的計數給 $d(x,y)$。[此確實為真對所有 $n\in\mathbf{Z}^+$，所以 $\text{wt}(x+y)=d(x,y)$ 對所有 x，$y\in\mathbf{Z}_2^n$。]

當 x，$y\in\mathbf{Z}_2^n$ 時，我們記 $d(x,y)=\sum_{i=1}^{n}d(x_i,y_i)$，其中，

對每個 $1\le i\le n$，$d(x_i,y_i)=\begin{cases}0 & \text{若 } x_i=y_i\\ 1 & \text{若 } x_i\neq y_i\end{cases}$。

引理 16.2 對所有 x，$y \in \mathbf{Z}_2^n$，$\text{wt}(x+y) \le \text{wt}(x)+\text{wt}(y)$。

證明： 我們以分別檢視，對每個 $1 \le i \le n$，x，y，$x+y$ 的所有分量 x_i，y_i，x_i+y_i 來證明這個引理。僅有一種情況將導致這個不等式失敗：若 $x_i+y_i=1$ 而 $x_i=0$ 且 $y_i=0$，對某些 $1 \le i \le n$。但此從未發生，因為 $x_i+y_i=1$ 蘊涵 x_i 和 y_i 中恰有一個是 1。

在例題 16.22 中，我們發現

$$\text{wt}(x+y)=\text{wt}(10100)=2 \le 2+4=\text{wt}(01001)+\text{wt}(11101)=\text{wt}(x)+\text{wt}(y)。$$

定理 16.11 定義在 $\mathbf{Z}_2^n \times \mathbf{Z}_2^n$ 上的距離函數 d 滿足下面，對所有 x，y，$z \in \mathbf{Z}_2^n$。

(a) $d(x, y) \ge 0$　　(b) $d(x, y)=0 \Leftrightarrow x=y$

(c) $d(x, y)=d(y, x)$　　(d) $d(x, z) \le d(x, y)+d(y, z)$

證明： 我們留前三個結果給讀者而證明 (d)。

在 $\mathbf{Z}_2^n$ 上，$x+y=0$，所以 $d(x, z)=\text{wt}(x+z)=\text{wt}(x+(y+y)+z)=\text{wt}((x+y)+(y+z)) \le \text{wt}(x+y)+\text{wt}(y+z)$，由引理 16.2，以 $\text{wt}(x+y)=d(x, y)$ 且 $\text{wt}(y+z)=d(y, z)$，結果成立。(此性質一般被稱是**三角不等式** (Triangle Inequality。)

當一個函數滿足定理 16.11 所列的四個性質時，它被稱是一個**距離函數** (distance function) 或**度量** (metric) 且我們稱 $(\mathbf{Z}_2^n, d)$ 是一個**度量空間** (metric space)。因此 d (如上所給) 經常被稱是 **Hamming 度量** (Hamming metric)。這個度量被使用於下面。

定義 16.10 對 n，$k \in \mathbf{Z}^+$ 且 $x \in \mathbf{Z}_2^n$，中心在 x 半徑為 k 的**球** (sphere) 被定義為 $S(x, k)=\{y \in \mathbf{Z}_2^n | d(x, y) \le k\}$。

例題 16.23 對 $n=3$ 且 $x=110 \in \mathbf{Z}_2^3$，$S(x, 1)=\{110, 010, 100, 111\}$ 且 $S(x, 2)=\{110, 010, 100, 111, 000, 101, 011\}$。

有這些預備知識在手，我們現在轉到本節的兩個主要結果。

定理 16.12 令 $E: W \to C$ 是一個編碼函數具訊息集 $W \subseteq \mathbf{Z}_2^m$ 及碼字集 $E(W)=C \subseteq \mathbf{Z}_2^n$，其中 $m<n$。若我們的目標是錯誤偵測，則對 $k \in \mathbf{Z}^+$，我們可偵測所有權數 $\le k$ 的傳送錯誤若且唯若碼字間的最小距離至少是 $k+1$。

證明：傳送者及接收者均知集合 C，所以若 $w \in W$ 是訊息且 $c = E(w)$ 被傳送，令 $c \neq T(c) = r$。若碼字間最小距離至少是 $k+1$，則 c 的傳送可導致 k 的錯誤之多且 r 將不被列在 C 裡。因我們可偵測所有錯誤 e，其中 $\text{wt}(e) \leq k$。反之，令 c_1，c_2 為碼字滿足 $d(c_1, c_2) < k+1$。則 $c_2 = c_1 + e$，其中 $\text{wt}(e) \leq k$。若我們傳送 c_1 且 $T(c_1) = c_2$，則我們將感覺 c_2 已被傳送，因此失敗偵測一個權數 $\leq k$ 的錯誤。

關於錯誤-修正的能力，我們能說什麼呢？

定理 16.13

令 E，W，和 C 如定理 16.12 的。若我們的目標是錯誤修正，則對 $k \in \mathbf{Z}^+$，我們可建構一個解碼函數 $D : \mathbf{Z}_2^n \to W$ 修正所有權數 $\leq k$ 的傳送錯誤若且唯若碼字間的最小距離是至少 $2k+1$。

證明：對 $c \in C$，考慮 $S(c, k) = \{x \in \mathbf{Z}_2^n | d(c, x) \leq k\}$。定義 $D : \mathbf{Z}_2^n \to W$ 如下：若 $r \in \mathbf{Z}_2^n$ 且 $r \in S(c, k)$ 對某些碼字 c，則 $D(r) = w$，其中 $E(w) = c$。[此處 c 是最靠近 r 的 (唯一) 碼字。] 若 $r \notin S(c, k)$ 對任意 $c \in C$，則我們定義 $D(r) = w_0$，其中 w_0 是某個任意訊息，其一旦被選上後即保持固定。這裡我們能面對的唯一問題是 D 可能不是一個函數。此將發生若存在一元素 $r \in \mathbf{Z}_2^n$ 滿足 r 同時在 $S(c_1, k)$ 及 $S(c_2, k)$ 上，對不同的碼字 c_1，c_2。但 $r \in S(c_1, k) \Rightarrow d(c_1, r) \leq k$，且 $r \in S(c_2, k) \Rightarrow d(c_2, r) \leq k$，所以 $d(c_1, c_2) \leq d(c_1, r) + d(r, c_2) \leq k + k < 2k+1$。因此，若碼字間的最小距離至少是 $2k+1$，則 D 是一個函數，且它將解碼所有可能接收的字，修正任意權數 $\leq k$ 的傳送錯誤。反之，若 c_1，$c_2 \in C$ 且 $d(c_1, c_2) \leq 2k$，則 c_2 可由 c_1 以最多 $2k$ 的改變獲得。以碼字 c_1 開始，我們做大約這些改變的一半 (正好是 $\lfloor d(c_1, c_2)/2 \rfloor$)。此帶給我們 $r = c_1 + e_1$，其中 $\text{wt}(e_1) \leq k$。由 r 繼續，我們做了剩餘的改變而得到 c_2 且發現 $r + e_2 = c_2$，其中 $\text{wt}(e_2) \leq k$。但則 $r = c_2 + e_2$。現在以 $c_1 + e_1 = r = c_2 + e_2$ 且 $\text{wt}(e_1)$，$\text{wt}(e_2) \leq k$，吾人如何可由 r 出現來決定碼字？這個模稜兩可的結果導致一個權數 $\leq k$ 的可能錯誤，其不可能被修正。

例題 16.24

以 $W = \mathbf{Z}_2^2$，令 $E : W \to \mathbf{Z}_2^6$ 為

$$E(00) = 000000 \quad E(10) = 101010 \quad E(01) = 010101 \quad E(11) = 111111.$$

則碼字間的最小距離是 3，所以我們可以修正所有的單一錯誤。

以

$$S(000000, 1) = \{x \in \mathbf{Z}_2^6 | d(000000, x) \le 1\}$$
$$= \{000000, 100000, 010000, 001000, 000100, 000010, 000001\},$$

解碼函數 $D : \mathbf{Z}_2^6 \to W$ 給 $D(x) = 00$ 對所有 $x \in S(000000, 1)$。

同理，

$$S(010101, 1) = \{x \in \mathbf{Z}_2^6 | d(010101, x) \le 1\}$$
$$= \{010101, 110101, 000101, 011101, 010001, 010111, 010100\},$$

且這裡 $D(x) = 01$ 對每個 $x \in S(010101, 1)$。此刻 D 的定義域佔有 $\mathbf{Z}_2^6$ 中的 14 個元素。繼續定義 D 給 $S(101010, 1)$ 及 $S(111111, 1)$ 的 14 個元素，剩下 36 個其它元素等待處理。我們定義 $D(x) = 00$ (或任意其它訊息) 給這 36 個其它元素且有一個解碼函數將修正單一錯誤。

注意！關於定理 16.12 及 16.13 有一個不可思議點需要處理。例如，若碼字間的最小距離是 $2k+1$，吾人可能感覺我們可以偵測所有權數 $\le 2k$ 的錯誤，且修正所有權數 $\le k$ 的錯誤。這未必為真。亦即，錯誤偵測及錯誤修正未必發生在同一時刻及在最大層次。欲看這個，再考慮例題 16.24 的 (6, 2) -三重重複碼。此時的編碼函數 $E : W (= \mathbf{Z}_2^2) \to \mathbf{Z}_2^6$ 被給為 $E(w_1w_2) = w_1w_2w_1w_2w_1w_2$ 且這個碼由 E 的值域中 $\mathbf{Z}_2^6$ 的四個元素組成。因為 $\mathbf{Z}_2^2$ 的任兩元素間的最小距離是 1，得碼字間的最小距離是 3 (如稍早在例題 16.24 所觀察的)。

現假設我們的主要目標是錯誤修正且 $r = 100000$ [$\notin E(w)$] 被接收。我們看到 $d(000000, r) = 1$，$d(101010, r) = 2$，$d(010101, r) = 4$，及 $d(111111, r) = 5$。因此，我們應選擇將 r 解碼為 000000，唯一最靠近 r 的碼字。不幸的，假設真正的訊息是 10 (對應碼字 101010)，但我們接收 $r = 100000$。一旦修正 r 為 000000，我們應接著解碼 000000 以得不正確訊息 00。且，依如此做，我們無法偵測一個權數為 2 的錯誤。

在這個型態的情況，吾人可發展一個格式，其中一個混合技巧被使用。此處錯誤修正及錯誤偵測兩者在某些層次可被實施。

對 $t \in \mathbf{N}$，若接收字為 r 且存在一個唯一碼字 c_1 滿足 $d(c_1, r) \le t$，則我們解碼 r 為 c_1。(注意：$r = c_1$ 的情形被覆蓋當 $t = 0$ 時。) 若存在第二個碼字 c_2 滿足 $d(c_2, r) = d(c_1, r)$，或若 $d(c, r) > t$ 對所有碼字 c，則一個錯誤被宣佈 (且再傳送被廣泛的要求)。使用這個格式，若碼字間最小距離至少是 $2t+s+1$，對 $s \in \mathbf{N}$。則我們可修正所有權數 $\le t$ 的錯誤，且偵測所有權數介於 $t+1$ (含) 及 $t+s$ (含) 之間的錯誤。

當使用這個格式給 (6, 2) -三重重複碼，我們的選擇包含：

1) $t=0$；$s=2$：這裡我們可偵測所有權數 ≤ 2 的錯誤，但我們沒有錯誤修正能力。
2) $t=1$；$s=0$：這裡單一錯誤被修正，但沒有錯誤-偵測能力。

若我們使用 (10, 2) -五次重複碼，則最小距離是 5。應用上面格式於這情形，我們的選擇現包含：

1) $t=0$；$s=4$：這裡我們可偵測所有權數 ≤ 4 的錯誤，但我們沒有錯誤修正能力。
2) $t=1$；$s=2$：現在單一錯誤被修正且我們亦可偵測所有錯誤 e，其中 $2 \le \text{wt}(e) \le 3$。
3) $t=2$；$s=0$：權數 ≤ 2 的所有錯誤被修正，但沒有錯誤-偵測能力。

[欲多瞭解這方面，有興趣的讀者應檢視 S.Roman [24] 的第 4 章。]

16.7　奇偶性-校驗及生成器矩陣

本節我們將介紹一個例子，其中編碼及解碼函數被給為佈於 $\mathbf{Z}_2$ 的矩陣。這些矩陣之一將助我們找出最近的碼字給一個已知的接受的字。這個將特別有幫助，當碼字集 C 變為大時。

例題 16.25

令

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

為佈於 $\mathbf{Z}_2$ 的 3×6 矩陣。G 的前三行形成 3×3 單位矩陣 I_3。令 A 為 G 的後三行所形成的矩陣，我們記 $G=[I_3|A]$ 來表它的結構。 (分割的) 矩陣 G 被稱是一個**生成器矩陣** (generator matrix)。

我們利用 G 來定義一個編碼函數 $E:\mathbf{Z}_2^3\to\mathbf{Z}_2^6$ 如下。對 $w\in\mathbf{Z}_2^3$，$E(w)=wG$ 是 $\mathbf{Z}_2^6$ 上的元素，其由乘 w 而得，被考慮為一個三-維列向量，以矩陣 G 在其右邊。不像第 7 章的矩陣乘法結果，在計算中，這裡我們有 $1+1=0$，而非 $1+1=1$。

(甚至若訊息集 W 不是 $\mathbf{Z}_2^3$ 的全部，我們將假設所有 $\mathbf{Z}_2^3$ 是編碼的且傳送者及接收者均知道真實的重要訊息及其對應的碼字。)

我們發現這裡，例如，

$$E(110) = (110)G = [110]\begin{bmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{bmatrix} = [110101],$$

及

$$E(010) = (010)G = [010]\begin{bmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{bmatrix} = [010011].$$

注意 $E(110)$ 可由將 G 的前兩列相加而得，而 $E(010)$ 即是 G 的第二列。

由這個方法得到的碼字集是

$$C = \{000000, 100110, 010011, 001101, 110101, 101011, 011110, 111000\} \subseteq \mathbf{Z}_2^6,$$

且吾人利用簡單的去掉碼字的後三分量，可取回對應的訊息。此外，碼字間的最小距離是 3，所以我們可偵測權數 ≤ 2 的錯誤或修正單一錯誤。(我們將假設多重錯誤很少且集中在錯誤修正。)

對所有 $w = w_1w_2w_3 \in \mathbf{Z}_2^3$，$E(w) = w_1w_2w_3w_4w_5w_6 \in \mathbf{Z}_2^6$。因為

$$\begin{aligned}E(w) &= [w_1w_2w_3]\begin{bmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&0&1\end{bmatrix}\\ &= [w_1w_2w_3(w_1+w_3)(w_1+w_2)(w_2+w_3)],\end{aligned}$$

我們有 $w_4 = w_1 + w_3$，$w_5 = w_1 + w_2$，$w_6 = w_2 + w_3$，且這些方程式被稱是**奇偶性-校驗方程式** (parity-check equations)。因為 $w_i \in \mathbf{Z}_2$ 對每個 $1 \leq i \leq 6$，得 $w_i = -w_i$，且所以方程式可被改寫為

$$\begin{aligned}w_1 \quad &+ w_3 + w_4 &&= 0\\ w_1 + w_2 \quad &+ w_5 &&= 0\\ w_2 + w_3 \quad &+ w_6 &&= 0.\end{aligned}$$

因此我們發現

$$\begin{bmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}w_1\\w_2\\w_3\\w_4\\w_5\\w_6\end{bmatrix} = H\cdot(E(w))^{\text{tr}} = \begin{bmatrix}0\\0\\0\end{bmatrix},$$

其中 $(E(w))^{\text{tr}}$ 表 $E(w)$ 的轉置。因此，若 $r = r_1r_2\cdots r_6 \in \mathbf{Z}_2^6$，我們辨認 r 為一

個碼字若且唯若

$$H \cdot r^{\text{tr}} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

記得 $H=[B|I_3]$，我們注意若 B 的所有列和行互換，則得 A。因此 $B=A^{\text{tr}}$。

由稍早在誤差修正所發展的理論，因為本例題碼字間的最小距離為 3，我們應能發展一個解碼函數來修正單一錯誤。

假設我們接收 $r=110110$。我們想找碼字 c，其為 r 的最近之鄰居。若有一長串的碼字反對校驗 r，我們最好首先檢視 $H \cdot r^{\text{tr}}$，其被稱為 r 的**特徵** (syndrome)。此處

$$H \cdot r^{\text{tr}} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix},$$

所以 r 不是一個碼字。因此，我們至少偵測一個錯誤。回看碼字表列，我們看到 $d(100110, r)=1$。對所有其它 $c \in C$，$d(r, c) \geq 2$。記 $r=c+e=100110+010000$，我們發現 (權數 1 的) 傳送誤差發生在 r 的第二個分量。特徵 $H \cdot r^{\text{tr}}$ 產生 H 的第二行僅是一個巧合嗎？若否，則我們可利用這個結果以便瞭解若一個單一傳送錯誤發生，它發生在第二個分量。改變 r 的第二個分量，我們得到 c；訊息 w 由 c 的前三個分量所組成。

令 $r=c+e$，其中 c 是一個碼字且 e 是一個權數為 1 的錯誤型。假設 1 是在 e 的第 i 個分量，其中 $1 \leq i \leq 6$，則

$$H \cdot r^{\text{tr}} = H \cdot (c+e)^{\text{tr}} = H \cdot (c^{\text{tr}} + e^{\text{tr}}) = H \cdot c^{\text{tr}} + H \cdot e^{\text{tr}}.$$

由於 c 是一個碼字，得 $H \cdot c^{\text{tr}}=\mathbf{0}$，所以 $H \cdot r^{\text{tr}}=H \cdot e^{\text{tr}}=$ 矩陣 H 的第 i 行。因此，c 和 r 僅差異在第 i 個分量，且我們可以簡單的改變 c 的第 i 分量來決定 c。

因為我們主要關心很少有多重錯誤的傳送，這個技巧是有限定的。若我們要求多一點，然而，我們將發現我們期望太多了。

假設我們接收 $r=000111$。計算特徵

$$H \cdot r^{\text{tr}} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

我們得到一個不是 H 之行的結果。$H \cdot r^{\text{tr}}$ 可被獲得為 H 的兩行之和。若 $H \cdot r^{\text{tr}}$ 來自 H 的第一及第六行，則修正 r 上的這些分量，得到碼字 100110。若我們將 H 的第三及第五行相加來得這個特徵，一旦改變 r 的第三及第五個分量，我們得第二個碼字，001101。所以我們不能期望 H 來修正多重錯誤。這沒什麼好驚奇的，因為碼字間的最小距離是 3。

我們將例題 16.25 的結果總結為一般情形。對 m，$n \in \mathbf{Z}^+$，其中 $m < n$，編碼函數 $E : \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ 以一個佈於 $\mathbf{Z}_2$ 的 $m \times n$ 矩陣 G 來給之。這個矩陣 G 被稱是碼的生成器矩陣且其形式為 $[I_{m1} | A]$，其中 A 是一個 $m \times (n - m)$ 矩陣。此處 $E(w) = wG$，對每個訊息 $w \in \mathbf{Z}_2^m$，且碼 $C = E(\mathbf{Z}_2^m) \subset \mathbf{Z}_2^n$。

所結合的**奇偶性-校驗矩陣** (parity-check matrix) H 是一個形式為 $[A^{\text{tr}} | I_{n\ \ m}]$ 的 $(n - m) \times n$ 矩陣。這個矩陣亦可被用來定義編碼矩陣 E，因為若 $w = w_1 w_2 \cdots w_m \in \mathbf{Z}_2^m$，則 $E(w) = w_1 w_2 \cdots w_m w_{m+1} \cdots w_n$，其中 $w_{m+1}, \cdots, w_n$ 可由 $H \cdot (E(w))^{\text{tr}} = \mathbf{0}$ 所產生的 $n - m$ 個 (奇偶性-校驗) 方程式集，$n - m$ 個 0 的行向量，來決定。

這個唯一的奇偶性-校驗矩陣 H 亦提供一個解碼格式，其可修正傳送中的單一錯誤若：

a) H 不含一個均為 0 的行。 (若 H 的第 i 行全為 0 且 $H \cdot r^{\text{tr}} = \mathbf{0}$ 對一個接收的字 r，我們不能決定 r 是否是一個碼字或是一個接收字，其第 i 個分量被不正確傳送。我們不想將 r 和所有碼字做比較當 C 是大的時候。)

b) H 中沒兩行是相同的。 (若 H 的第 i 及第 j 行相同且 $H \cdot r^{\text{tr}}$ 等於這個重複行，我們將如何決定 r 的哪一分量要改變呢？)

當 H 滿足這兩個條件時，我們得到下面解碼演算法。對每個 $r \in \mathbf{Z}_2^n$，若 $T(c) = r$，則：

1) 以 $H \cdot r^{\text{tr}} = \mathbf{0}$，我們感覺到傳送是正確的且 r 是被傳送的碼字。解碼訊息則由 r 的前 m 個分量所組成。

2) 以 $H \cdot r^{tr}$ 等於 H 的第 i 行，我們感覺到傳送中有一個單一錯誤且改變 r 的第 i 個分量以得碼字 c。此時 c 的前 m 個分量產生原始訊息。
3) 若情形 1 及情形 2 均不發生，我們感覺到有多於一個傳送錯誤且我們無法提供一個可信賴的方法來解這個情形的碼。

我們以矩陣 H 上的最後一個建議來結束本章。若我們以一個奇偶性-校驗矩陣 $H=[B|I_{n\ \ m}]$ 開始且使用它，如上面所描述的，來定義函數 E，則我們得到相同的碼字集，其係由所結合的生成器矩陣 $G=[I_m|B^{tr}]$ 所生成的。

習題 16.6 及 16.7

1. 對例題 16.24，列出 $S(101010, 1)$ 及 $S(111111, 1)$ 的所有元素。
2. 解碼下面由例題 16.24 所接收的各個字。
   a) 110101　　b) 101011
   c) 001111　　d) 110000
3. a) 若 $x \in \mathbf{Z}_2^{10}$，求 $|S(x, 1)|$，$|S(x, 2)|$，$|S(x, 3)|$。
   b) 對 n，$k \in \mathbf{Z}^+$ 滿足 $1 \le k \le n$，若 $x \in \mathbf{Z}_2^n$，則 $|S(x, k)|$ 值為何？
4. 令 $E : \mathbf{Z}_2^5 \to \mathbf{Z}_2^{25}$ 是一個編碼函數，其碼字間的最小距離是 9，我們可偵測權數 $\le k$ 之錯誤的最大 k 值是多少？若我們想修正權數 $\le n$ 之錯誤，則 n 的最大值為何？
5. 對下面各個編碼函數，求碼字間的最小距離。討論各個碼的錯誤偵測及錯誤修正可能性。
   a) $E : \mathbf{Z}_2^2 \to \mathbf{Z}_2^5$
      00 → 00001　　01 → 01010
      10 → 10100　　11 → 11111
   b) $E : \mathbf{Z}_2^2 \to \mathbf{Z}_2^{10}$
      00 → 0000000000　　01 → 0000011111
      10 → 1111100000　　11 → 1111111111
   c) $E : \mathbf{Z}_2^3 \to \mathbf{Z}_2^6$
      000 → 000111　　001 → 001001
      010 → 010010　　011 → 011100
      100 → 100100　　101 → 101010
      110 → 110001　　111 → 111000
   d) $E : \mathbf{Z}_2^3 \to \mathbf{Z}_2^8$
      000 → 00011111　　001 → 00111010
      010 → 01010101　　011 → 01110000
      100 → 10001101　　101 → 10101000
      110 → 11000100　　111 → 11100011
6. a) 利用例題 16.25 的奇偶性-校驗矩陣 H，解碼下面各個接收字。
      i) 111101　　ii) 110101
      iii) 001111　　iv) 100100
      v) 110001　　vi) 111111
      vii) 111100　　viii) 010100
   b) (a) 的所有結果是被唯一決定的嗎？
7. 編碼函數 $E : \mathbf{Z}_2^2 \to \mathbf{Z}_2^5$ 以生成器矩陣來給之。

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

   a) 決定所有碼字。這個碼的錯誤偵測可

能性是什麼？錯誤修正可能性是什麼？

b) 找所結合的奇偶性-校驗矩陣 H。

c) 利用 H 來解碼下面各個接收字。

i) 11011　ii) 10101　iii) 11010

iv) 00111　v) 11101　vi) 00110

8. 以奇偶性-校驗矩陣來定義編碼函數 $E: \mathbf{Z}_2^3 \to \mathbf{Z}_2^6$。

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

a) 決定所有碼字。

b) 這個碼能修正傳送中的所有單一錯誤嗎？

9. 求生成器及奇偶性-校驗矩陣給例題 16.20 的 (9, 8) 單一奇偶性-校驗編碼格式。

10. a) 證明 1×9 矩陣 $G = [1 \quad 1 \quad 1 \cdots 1]$ 是 (9, 1) 九次重複碼的生成矩陣。

b) 這情形所結合的奇偶性-校驗矩陣 H 為何？

11. 對一個具有生成器矩陣 $G = [I_m | A]$ 及奇偶性-校驗矩陣 $H = [A^{tr} | I_{n-m}]$，含生成器矩陣 $[I_{n-m} | A^{tr}]$ 及奇偶性-校驗矩陣 $[A | I_m]$ 的 $(n, n-m)$ 碼 C^d 被稱是 C 的**對偶碼** (dual code)。證明習題 9 及 10 的各個碼構成一對一對偶碼。

12. 給 $n \in \mathbf{Z}^+$，令集合 $M(n, k) \subseteq \mathbf{Z}_2^n$ 包含長度為 n 的碼字的最大數，其中碼字間的最小距離是 $2k+1$。證明

$$\frac{2^n}{\sum_{i=0}^{2k} \binom{n}{i}} \le |M(n, k)| \le \frac{2^n}{\sum_{i=0}^{k} \binom{n}{i}}.$$

($|M(n, k)|$ 的上界被稱是 **Hamming 界** (Hamming bound)；下界被稱是 **Gilbert 界** (Gilbert bound)。

16.8　群碼：以傍集首項解碼

我們已檢視一些編碼理論的導引教材，現在是看看群結構如何進入這個領域的時候。

定義 16.11

令 $E: \mathbf{Z}_2^m \to \mathbf{Z}_2^n$，其中 $n > m$，為一編碼函數。碼 $C = E(\mathbf{Z}_2^m)$ 被稱是一個**群碼** (group code) 若 C 是 $\mathbf{Z}_2^n$ 的一個子群。

記得 (例題 16.24 的) 編碼函數 $E: \mathbf{Z}_2^2 \to \mathbf{Z}_2^6$，其中

$$E(00) = 000000 \quad E(10) = 101010 \quad E(01) = 010101 \quad E(11) = 111111.$$

在各分量相加模 2 之下，此處 $\mathbf{Z}_2^2$ 及 $\mathbf{Z}_2^6$ 為群；子集合 $C = E(\mathbf{Z}_2^2) = \{000000, 101010, 010101, 111111\}$ 是 $\mathbf{Z}_2^6$ 的一個子群，且是一個群碼的例子。 (注意

C 包含 000000，$\mathbf{Z}_2^6$ 的零元素。)

一般來講，當碼字形成一個群時，我們發現比較容易來算碼字間的最小距離。

定理 16.14

在一個群碼裡，相異碼字間的最小距離是碼的非零元素中最小的權數。

證明：令 a，b，$c \in C$，其中 $a \neq b$，$d(a, b)$ 是最小值，且 c 是具最小權數的非零元素。由於群 C 的封閉性，$a+b$ 是一個碼字。因為 $d(a, b)=\text{wt}(a+b)$，由於 c 的選擇，我們有 $d(a, b) \geq \text{wt}(c)$。而且，$\text{wt}(c)=d(c, \mathbf{0})$，其中 $\mathbf{0}$ 是一個碼字，這是因為 C 是一個群。接著由於 a，b 的選擇，$d(c, \mathbf{0}) \geq d(a, b)$，所以 $\text{wt}(c) \geq d(a, b)$。因此，$d(a, b) = \text{wt}(c)$。

若 C 是一個碼字集且 $|C|=1024$，則我們必須計算 $\binom{1024}{2}=523{,}776$ 個距離來求碼字間的最小距離。但若我們可辨識 C 具有一個群結構，我們僅須計算 C 的 1023 個非零元素的權數即可。

是否有一些方法來保證碼字形成一個群？由定理 16.5(d)，一個子群的同態像是一個子群，所以若 $E: \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ 是一個群同態函數，則 $C=E(\mathbf{Z}_2^m)$ 將是 $\mathbf{Z}_2^n$ 的一個子群。我們的下一個結果將使用這個事實來證明我們使用一個生成器矩陣 G 或一個奇偶性-檢驗矩陣 H 所得到的碼是群碼。更而，此結果之證明再次確認我們 (在前節末) 對來自一個生成器矩陣 G 或其所結合的奇偶性-校驗矩陣 H 的碼所做的觀察。

定理 16.15

令 $E: \mathbf{Z}_2^m \to \mathbf{Z}_2^n$ 為由一個生成器矩陣 G 或其所結合的奇偶性-校驗矩陣 H 所給的編碼函數，則 $C=E(\mathbf{Z}_2^m)$ 是一個群碼。

證明：我們以證明來自 G 或 H 的函數 E 是一個群同態函數來證明這些結果。

若 x，$y \in \mathbf{Z}_2^m$，則 $E(x+y)=(x+y)G=xG+yG=E(x)+E(y)$。因此，$E$ 是一個同態函數且 $C=E(\mathbf{Z}_2^m)$ 是一個群碼 [由定理 16.5(d)]。

對於 H 的情形，若 x 是一個訊息，則 $E(x)=x_1x_2\cdots x_m x_{m\ 1}\cdots x_n$，其中 $x=x_1x_2\cdots x_m \in \mathbf{Z}_2^m$ 且 $H \cdot (E(x))^{\text{tr}}=\mathbf{0}$。特別地，$E(x)$ 被這兩個性質唯一決定。若 y 亦是一個訊息，則 $x+y$ 是一個訊息且 $E(x+y)$ 有 (x_1+y_1)，(x_2+y_2)，$\cdots$，(x_m+y_m) 為其前 m 個分量，如同 $E(x)+E(y)$。更而，$H \cdot (E(x)+E(y))^{\text{tr}}=H \cdot (E(x)^{\text{tr}}+E(y)^{\text{tr}})=H \cdot E(x)^{\text{tr}}+H \cdot E(y)^{\text{tr}}=\mathbf{0}+\mathbf{0}=\mathbf{0}$。因為 $E(x+y)$ 是 $\mathbf{Z}_2^n$ 上的唯一元素滿足 (x_1+y_1)，(x_2+y_2)，$\cdots$，(x_m+y_m) 為其前 m 個分量滿足 $H \cdot (E(x+y)^{\text{tr}}=\mathbf{0}$，得 $E(x+y)=E(x)+E(y)$。所以 E 是一個群同態

函數，且因此，$C=\{c \in \mathbf{Z}_2^n | H \cdot c^{\text{tr}} = \mathbf{0}\}$ 是一個群碼。

現在我們使用 C 的群結構，及其在 $\mathbf{Z}_2^n$ 的傍集，來發展一個解碼格式。我們的例題使用例題 16.25 所發展的碼，但程序應用給每個群碼。

例題 16.26

我們發展一個解碼表如下。

1) 首先以單位元素開始，將群碼 C 的所有元素列成一列。

000000 100110 010011 001101 110101 101011 011110 111000.

2) 其次選 $\mathbf{Z}_2^6$ (一般是 $\mathbf{Z}_2^n$) 上的一個元素 x，其中 x 目前不出現在所發展的表之任何地方且有最小權數。接著列出傍集 $x+C$ 的所有元素，且 $x+c$ 直接在 c 的下方，對每個 $c \in C$。對 $x=100000$，我們有

000000 100110 010011 001101 110101 101011 011110 111000
100000 000110 110011 101101 010101 001011 111110 011000.

3) 重複步驟 (2) 直到傍集提供 $\mathbf{Z}_2^6$ (一般是 $\mathbf{Z}_2^n$) 的一個分割。此得到表 16.8 所示的**解碼表** (decoding table)。
4) 一旦解碼表被建構，對各個接收字 r，我們找含 r 的行，並使用該行頂端的碼字 c 的前三個分量來解碼 r。

表 16.8　例題 16.25 的碼之解碼表

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

由表中，我們發現接收字

$$r_1=101001 \quad r_2=111010 \quad r_3=001001 \quad r_4=111011$$

的碼字分別為

$$c_1=101011 \quad c_2=111000 \quad c_3=001101 \quad c_4=101011.$$

由這些結果，得個別訊息為

$$w_1 = 101 \quad w_2 = 111 \quad w_3 = 001 \quad w_4 = 101.$$

表 16.8 第一行的所有元素被稱是**傍集首項** (coset leaders)。對前七列，所有表中的傍集首項均相同，其中可能有某些列的排列。然而，最後一列，不是 100001 或 001010 可已被使用來代替 010100，因為它們亦有最小權數 2。所以表未必唯一。[所以，並非所有兩個錯誤可被修正，因為對每個在最後傍集 (傍集首項為 010100 的傍集) 的 r 的最小距離，可能沒有唯一的碼。例如，$r = 001010$ 有三個最近的碼字 (在距離 2) ——即，000000，101011，及 011110。]

傍集首項如何真正的幫助我們？第一列的碼字似乎是我們在上面用來解碼 r_1，r_2，r_3，及 r_4 的碼字。

考慮第六列的接收字 $r_1 = 101001$ 及 $r_2 = 111010$，其中傍集首項是 $x = 00010$。計算特徵，我們發現

$$H \cdot (r_1)^{\text{tr}} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = H \cdot (r_2)^{\text{tr}} = H \cdot x^{\text{tr}}.$$

這不只是一個巧合。

定理 16.16　令 $C \subseteq \mathbf{Z}_2^n$ 是一個群碼對一個奇偶性-校驗矩陣 H，且令 r_1，$r_2 \in \mathbf{Z}_2^n$。對 C 在 $\mathbf{Z}_2^n$ 上的傍集表，r_1 及 r_2 位在相同的 C 之傍集若且唯若 $H \cdot (r_1)^{\text{tr}} = H \cdot (r_2)^{\text{tr}}$。

證明：若 r_1 及 r_2 位在相同傍集，則 $r_1 = x + c_1$ 及 $r_2 = x + c_2$，其中 x 是傍集首項，且 c_1 和 c_2 分別是位在 r_1 及 r_2 之行頂端的碼字。則 $H \cdot (r_1)^{\text{tr}} = H \cdot (x + c_1)^{\text{tr}} = H \cdot x^{\text{tr}} + H \cdot c_1^{\text{tr}} = H \cdot x^{\text{tr}} + \mathbf{0} = H \cdot x^{\text{tr}}$，因為 c_1 是一個碼字。同樣的，$H \cdot (r_2)^{\text{tr}} = H \cdot x^{\text{tr}}$，所以 r_1，r_2 有相同的特徵。反之 $H \cdot (r_1)^{\text{tr}} = H \cdot (r_2)^{\text{tr}} \Rightarrow H \cdot (r_1 + r_2)^{\text{tr}} = \mathbf{0} \Rightarrow r_1 + r_2$ 是一個碼字 c。因此 $r_1 + r_2 = c$，所以 $r_1 = r_2 + c$ 且 $r_1 \in r_2 + C$。因為 $r_2 \in r_2 + C$，我們有 r_1，r_2 在相同的傍集裡。

在解碼接收字時，當表 16.8 被使用時，我們必須搜尋 64 個元素來找一個已給的接收字。對 $C \subseteq \mathbf{Z}_2^{12}$，共有 4096 個串，每一個串有 12 位元。此一個搜尋過程是繁厭的，所以或許我們應考慮有一個電腦來做搜尋。目前這個工具儲存整個表：表 16.8 需 $6 \times 64 = 384$ 儲存位元；對 $C \subseteq \mathbf{Z}_2^{12}$ 需 $12 \times 4096 = 49{,}152$ 個位元。我們應喜歡來改進這個情況。然而，在事情變得更好前，它將看起來更差，當我們將表 16.8 擴大為表 16.9 所示的時。

表 16.9　含特徵的解碼表 16.8

000	000000	100110	010011	001101	110101	101011	011110	111000
110	100000	000110	110011	101101	010101	001011	111110	011000
011	010000	110110	000011	011101	100101	111011	001110	101000
101	001000	101110	011011	000101	111101	100011	010110	110000
100	000100	100010	010111	001001	110001	101111	011010	111100
010	000010	100100	010001	001111	110111	101001	011100	111010
001	000001	100111	010010	001100	110100	101010	011111	111001
111	010100	110010	000111	011001	100001	111111	001010	101100

這個新表包含傍集首項左邊的各列特徵 (之轉置)。

現在我們可以下面程序來解碼接收字 r。

1) 計算特徵 $H \cdot r^{\text{tr}}$。
2) 在 $H \cdot r^{\text{tr}}$ 的右邊找傍集首項 x。
3) 將 x 加至 r 以得 c。(在含 r 的行之頂端，我們正在尋找的碼字 c 滿足 $c+x=r$，或 $c=x+r$。)

因此，表 16.9 中所有需要的是前兩行，其將需要 (3)(8) +(6)(8) = 72 個儲存位元。以多 18 個儲存位元給 H，我們可儲存解碼過程所需的東西於 90 個儲存位元裡，稱此過程為**以傍集首項解碼** (decoding by coset leaders)，而不是原先估計的 384 位元。

應用此過程至 $r=110110$，我們發現

$$H \cdot r^{\text{tr}} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

因為 011 位在傍集首項 $x=010000$ 的左邊，碼字 $c=x+r=010000+110110=100110$，由此我們取回原始訊息，100。

這裡的碼是一個群碼，其中所有非零碼字的最小權數是 3，所以我們期待能找一個解碼格式來修正單一錯誤。在這裡這是可達成的，因為權數為 1 的錯誤型是一個傍集首項，在我們的解碼格式可在傳送中修正單一及雙重錯誤兩者前，所有權數為 1 或為 2 的錯誤型將必是傍集首項。

不像例題 16.25 的情況，其中特徵亦被使用給解碼，這裡的狀況有點不同。一旦我們有一個完整的表來列出 C 在 $\mathbf{Z}_2^6$ 的所有傍集，利用傍集首項的解碼過程將給我們一個答案給所有接收字，不僅給碼字或有特徵出現在奇偶性-校驗矩陣 H 的行中。然而，我們確實明白這裡仍舊有一個問題，因為我們的表的最後一列不是唯一的。但是，當我們的最後結果將斷

言，這個方法提供一個解碼格式，其和其它格式一樣好。

定理 16.17

當我們正在利用傍集首項解碼時，若 $r \in \mathbf{Z}_2^n$ 是一個接收字且 r 被解碼為碼字 c^* (我們解碼它以取回訊息)，則 $d(c^*, r) \le d(c, r)$ 對所有碼字 c。

證明：令 x 為傍集首項給包含 r 的傍集。則 $r = c^* + x$，或 $r + c^* = x$，所以 $d(c^*, r) = \text{wt}(r + c^*) = \text{wt}(x)$。若 c 是任意碼字，則 $d(c, r) = \text{wt}(c + r)$，且我們有 $c + r = c + (c^* + x) = (c + c^*) + x$。因為 C 是一個群碼，得 $c + c^* \in C$ 且所以 $c + r$ 在傍集 $x + C$ 裡。在傍集 $x + C$ 的所有元素中，傍集每項 x 被選為具最小的權數，所以 $\text{wt}(c + r) \ge \text{wt}(x)$。因此，$d(c^*, r) = \text{wt}(x) \le \text{wt}(c + r) = d(c, r)$。

16.9　Hamming 矩陣

我們發現在修正傳送中單一錯誤方面，奇偶性-校驗矩陣 H 是有幫助的，若 (a) H 沒有全為 0 的行及 (b) H 中沒有兩行是相同的。對矩陣

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

我們發現 H 滿足這兩個條件，且對 H 中的列數 ($r = 3$) 我們可能有最大的行數。若加上一個額外的行，H 對修正單一錯誤將不再有用。

結合 H 的生成器矩陣 G 是

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

因此，我們有一個 (7, 4) 群碼。編碼函數 $E : \mathbf{Z}_2^4 \to \mathbf{Z}_2^7$ 將 4-位元訊息編碼為 7- 位元碼字。我們明白因為 H 是由三個奇偶性-校驗方程所決定的，我們現在有我們在訊息中能有的最大位元數 (在我們目前的編碼格式下)。而且，H 的所有行，由上讀到底，是由 1 到 7 的整數之二元等價。

一般來講，若我們以 r 個奇偶性-校驗方程開始，且奇偶性-校驗矩陣 H 可有 $2^r - 1$ 個行且仍舊被用來修正單一錯誤。在這些背景下，$H = [B|I_r]$，其中 B 是一個 $r \times (2^r - 1 - r)$ 矩陣，且 $G = [I_m|B^{\text{tr}}]$，其中 $m = 2^r - 1 - r$。依這個方去，奇偶性-校驗矩陣 H 結合一個 $(2^r - 1, 2^r - 1 - r)$ 群碼，H 被稱是一個 Hamming **矩陣** (Hamming matrix)，且這個碼被稱為

Hamming**碼** (Hamming code)。

例題 16.27

若 $r=4$，則 $2^r-1=15$ 且 $2^r-1-r=11$。對 $r=4$，一個 (直到一個行的排列) 可能 Hamming 矩陣 H 是

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

再次，H 的所有行包含由 1 到 15 ($=2^4-1$) 的整數的二元等價。

這個矩陣 H 是一個 Hamming (15, 11) 碼的奇偶性-校驗矩陣，Hamming (15, 11) 的速率是 11/15。

不管這些 Hamming 碼的速率，對所有 $r \geq 2$，此類碼的速率 m/n 被給為 $m/n=(2^r-1-r)/(2^r-1)=1-[r/(2^r-1)]$。當 r 增加時，$r/(2^r-1)$ 趨近 0 且速率趨近 1。

我們以一個最後觀察來結束編碼理論的討論。在 16.7 節，我們呈現 G (及 H) 於所謂的**系統型** (systematic form)。這些矩陣的所有列和行的其它安排亦是可能的，且這些產生**等價碼** (equivalent codes)。 (關於這個的更多材料可被發現於 L. L. Dornhoff 及 F. E. Hohn [4] 的書裡。) 我們在這裡提到這個是因為經常練習列出一個有 r 列的 Hamming 矩陣的所有行，使得由 1 到 2^r-1 的整數之二元表示式出現為 H 的所有行，且由左讀到右。對 Hamming (7, 4) 碼，本節一開始所提的矩陣 H 將取 (等價) 型

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

此處單位元素出現在第一、第二，及第四行以取代最後三行的單位元素。因此，我們將使用這些分量給奇偶性-校驗，且發現若我們送出訊息 $w=w_1w_2w_3w_4$，則對應的碼字 $E(w)$ 是 $c_1c_2w_1c_3w_2w_3w_4$，其中

$$\begin{aligned} c_1 &= w_1 + w_2 \qquad + w_4 \\ c_2 &= w_1 \qquad + w_3 + w_4 \\ c_3 &= \qquad w_2 + w_3 + w_4, \end{aligned}$$

使得 $H_1 \cdot (E(w))^{\text{tr}}=0$

特別地，若我們送出訊息 $w=w_1w_2w_3w_4=1010$，所對應的碼字將為 $E(w)=c=c_1c_2w_1c_3w_2w_3w_4=c_1c_21c_3010$，其中 $c_1=w_1+w_2+w_4=1+0+0=1$，$c_2=w_1+w_3+w_4=1+1+0=0$，且 $c_3=w_2+w_3+w_4=0+1+0=1$。則 c

$=1011010$ 且 $H_1 \cdot (E(w))^{tr} = H_1 \cdot (E(1010))^{tr} = H_1 \cdot (1011010)^{tr} = \mathbf{0}$。(證明之！) 所以若 $c=1011010$ 被送出，但 $r=1001010$ 被收到，我們有 $H_1 \cdot r^{tr} = H_1 \cdot (1001010)^{tr} = (011)^{tr}$。(亦證明之！) 因為 011 是 3 的二元表示式，我們知道錯誤是在位置 3 ——且此次我們並沒有檢視 H_1 的所有行。所以使用一個 H_1 型的奇偶性-校驗矩陣將簡化特徵解碼。一般來講，對 $c = c_1c_2w_1c_3w_2w_3w_4$，令 $r=c+e$，其中 e 是一個權數為 1 的錯誤型。且假設 e 中的 1 是在位置 i，其中 $1 \le i \le 7$，則特徵 $H_1 \cdot r^{tr}$ 提供 i 的二元表示式且我們可不必檢視 H_1 的所有行來決定 c。由 c 的第三、第五、第六，及第七分量，我們可取回原始訊息 w。

習題 16.8 及 16.9

1. 令 $E : \mathbf{Z}_2^8 \to \mathbf{Z}_2^{12}$ 是碼 C 的解碼函數。需要多少個計算來求碼字間的最小距離？若 E 是一個群同態函數，則需要多少個計算？
2. a) 使用表 16.9 來解碼下面各個接收字。

   000011　100011　111110　100001
   001100　011110　001111　111100

   b) 若使用一個不同的傍集首項集，(a) 中的任一結果有改變嗎？
3. a) 建構一個解碼表 (含特徵) 給由生成器矩陣所給的群碼。

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

   b) 使用 (a) 所得的表來解碼下面各個接收字。

   11110　11101　11011　10100
   10011　10101　11111　01100

   c) 這個碼能修正傳送中的單一錯誤嗎？
4. 令

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

   為一個 Hamming (7, 4) 碼的奇偶性-校驗矩陣。

   a) 編碼下面各個訊息：
   1000　1100　1011　1110　1001　1111.

   b) 解碼下面各個接收字：
   1100001　1110111　0010001　0011100.

   c) 建構一個由特徵及傍集首項所組成的解碼表給這個碼。

   d) 使用 (c) 的結果來解碼 (b) 中所給的接收字。
5. a) Hamming (63, 57) 碼的生成器矩陣大小為何？其所結合的奇偶性-校驗矩陣 H 的大小為何？

   b) 這個碼的速率是多少？
6. 比較 Hamming (7, 4) 碼及 (3, 1) 三重重複碼的速率。
7. a) 令 $p=0.01$ 是一個二元對稱頻道不正確傳送的機率。若訊息 1011 經由 Hamming (7, 4) 碼送出，則正確解碼的機率為何？

   b) 對一個 20- 位元訊息以五個長度為 4 的區組送出，回答 (a)。

16.10 計數及等價：Burnside 定理

在本節及下兩節，我們將發展一個著名的計數技巧，名叫 Polya 枚舉法。我們的發展將不是非常嚴謹的。我們將經常僅敘述理論的一般結果，如在解一個特殊問題中所見到的。我們使用這個計數技巧中所遇到的第一個問題型呈現於下面例題。

例題 16.28

我們有一組牙籤，每根牙籤的長度及顏色均相同，且有另一組圓塑膠盤。每個盤子有兩個洞，如圖 16.4 所示的，牙籤可被塞進去以形成不同形狀，例如一個正方形。 (見圖 16.5) 若每個圓盤不是紅色就是白色，則我們可形成多少個不同的正方形？

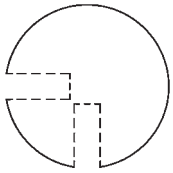


圖 16.4

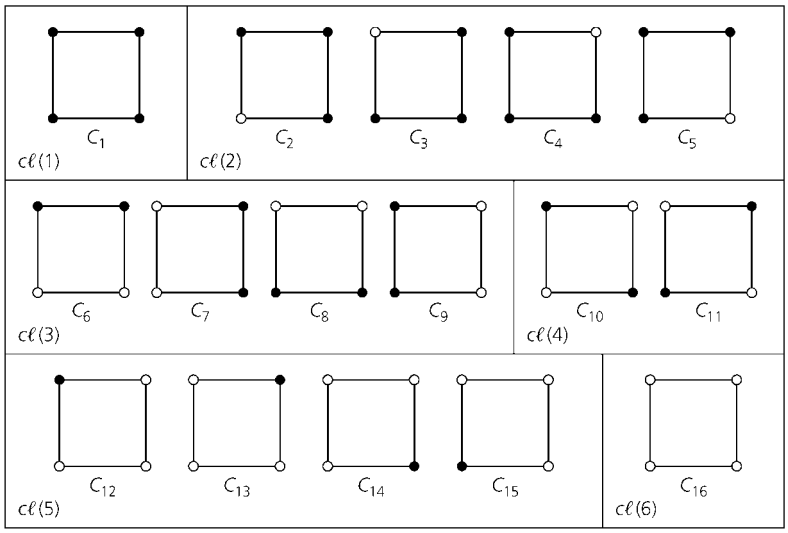


圖 16.5

若正方形被考慮為不動的，則 4 個圓盤位在 4 個不同的位置；紅色盤或白色盤被使用在各個位置。因此，有 $2^4=16$ 個不同圖案，如圖 16.5 所示，其中黑圓圈表示一個紅盤子。所有圖案被分成六類，$c\mathrm{l}(1)$，$c\mathrm{l}(2)$，…，$c\mathrm{l}(6)$，依據紅盤子的個數及相對位置。

現假設正方形不是固定的，但可在空中移動。除非頂點 (圓盤) 被做記號，圖 16.5 的某些圖案是無法區別的當我們移動它們時。

欲將這些觀念擺進更數學裡，我使用一個正方形的三維剛體運動之非交換群，來定義圖 16.5 中之圖案的一個等價關係，因為這個群將被使用

在本節及下兩節，我們現在給這個群的元素一個詳細的描述。

在圖 16.6，我們有群 $G=\{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$ 給 (a) 中正方形的剛體運動，其中我們將頂點標示為 1，2，3，及 4。(b) 經由圖 (i) 說明 G 的各個元素如何被應用。我們已將各個群元素表為 {1, 2, 3, 4} 的一個排列且在一個新型裡被稱是一個**互斥循環的乘積** (product of disjoint cycles)。例如，在 (b)，我們發現 $\pi_1=(1234)$。循環 (1234) 說明我們以 (a) 的正方形開始，在應用 π_1 後，我們發現 1 已被移到原先 2 所佔的位置，2 到 3 原先的位置，3 到 4 原先的位置，4 到 1 原先的位置。一般來講，若 xy 出現在一個循環裡，則 x 移到 y 原先所佔的位置。而且，對一個循環，其中 x 和 y 出現為 $(x\cdots y)$，y 移到 x 原先所佔的位置，當以這個循環所描述的運動被應用時。注意 $(1234)=(2341)=(3412)=(4123)$。我們說這些循環的每一個有**長度** 4，即為循環中元素的個數。在圖 (f) 中 r_1 的情

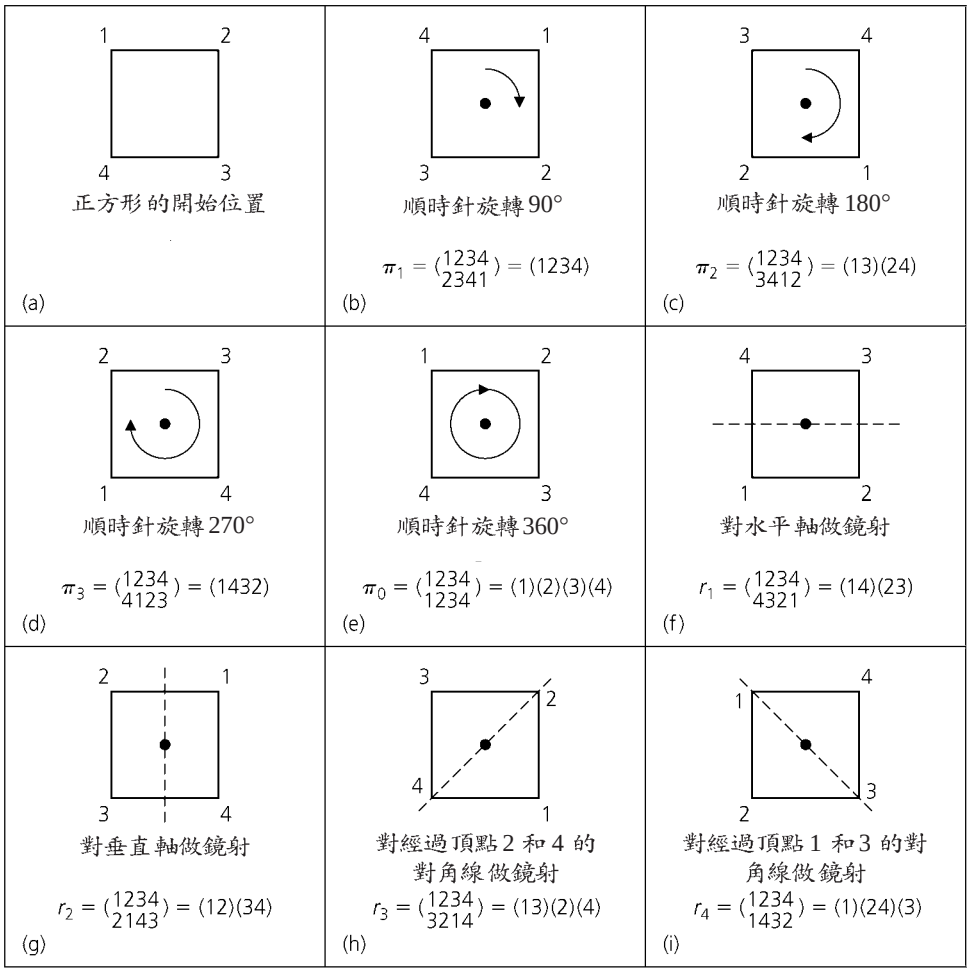


圖 16.6

形，以 1 開始，我們發現 r_1 將 1 送到 4，所以我們有 (14…) 作為 r_1 **分解** (decomposition) 中第一個循環的開始。然而，這裡的 r_1 將 4 送到 1，所以我們已完成完全分解的一部份——即 (14)。接著我們選一個尚未出現的頂點。例如，頂點 2。因為 r_1 送 2 到 3 且送 3 回到 2，所以我們得到第二個循環 (23)。此窮盡所有頂點且所以 (14)(23)＝r_1，其中循環 (14) 及 (23) 沒有共同頂點。此處 (14)(23)＝(23)(14)＝(23)(41)＝(32)(41) 均提供 r_1 的一個表示式為一個互斥循環的乘積，每個循環的長度為 2。最後，對群元素 r_3＝(13)(2)(4)，循環 (2) 說明 2 是固定的，或是不變的，在排列 r_3 之下。當所含的頂點個數為已知時，排列 r_3 亦可被表為 r_3＝(13)，其中消失的元素被理解為固定的。然而，我們將所有循環表於我們的分解中，因為這對我們稍後的討論是有用的。

在繼續討論圓盤和牙籤之前，讓我們檢視一些更進一步的互斥循環結果。

在 {1, 2, 3, 4, 5, 6} 的所有排列的群 S_6 中，令 $\pi=\begin{pmatrix}1&2&3&4&5&6\\2&3&1&4&6&5\end{pmatrix}$。做為一個互斥循環的乘積，

$$\pi_1=(123)(4)(56)=(56)(4)(123)=(4)(231)(65)\,.$$

若 $\sigma\in S_6$，且 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&4&5&1&6&3\end{pmatrix}$，則

$$\sigma=(124)(356)=\begin{pmatrix}1&2&3&4&5&6\\2&4&3&1&5&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\1&2&5&4&6&3\end{pmatrix},$$

所以每個循環可被認為是 S_6 的一個元素。

最後，若 α= (124)(3)(56) 且 β=(13)(245)(6) 為 S_6 的元素，則

$$\alpha\beta=(124)(3)(56)(13)(245)(6)=(143)(256)\,,$$

然而

$$\beta\alpha=(13)(245)(6)(124)(3)(56)=(132)(465)\,.$$

回到圖 16.5 的 16 個圖案或著色，我們現在檢視圖 16.6 的群 G 的每個元素如何作用在這些圖案上。例如，$\pi=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$ 依據圖 16.6(a) 中順時針旋轉正方形 90° 來排列 {1, 2, 3, 4}，而得圖 16.6(b) 的結果。此一旋轉如何作用在 $S=\{C_1, C_2, \cdots, C_{16}\}$，我們的著色集上呢？我們使用 π_1^* 來區分對 {1, 2, 3, 4} 的 90° 順時針旋轉及相同的旋轉應用至 $S=\{C_1, C_2,$

…, C_{16}}。 我們發現

$$\pi_1^* = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_3 & C_4 & C_5 & C_2 & C_7 & C_8 & C_9 & C_6 & C_{11} & C_{10} & C_{13} & C_{14} & C_{15} & C_{12} & C_{16} \end{pmatrix}.$$

作為一個互斥循環的乘積，

$$\pi_1^* = (C_1)(C_2C_3C_4C_5)(C_6C_7C_8C_9)(C_{10}C_{11})(C_{12}C_{13}C_{14}C_{15})(C_{16}).$$

我們注意到在 π_1^* 的作用下，沒有圖案被改變為另一類的圖案。

第二個例子，我們考慮圖 16.6(h) 的鏡射 r_3。這個在 S 上的剛體運動被給為

$$\begin{aligned} r_3^* &= \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_2 & C_5 & C_4 & C_3 & C_7 & C_6 & C_9 & C_8 & C_{10} & C_{11} & C_{14} & C_{13} & C_{12} & C_{15} & C_{16} \end{pmatrix} \\ &= (C_1)(C_2)(C_3C_5)(C_4)(C_6C_7)(C_8C_9)(C_{10})(C_{11})(C_{12}C_{14})(C_{13})(C_{15})(C_{16}). \end{aligned}$$

再次地，沒有圖案被 r_3^* 帶到原來這類之外的圖案。

使用**群 G 作用在集合 S 上** (the group G acting on the set S) 的概念，我們定義 S 上的一個關係 $\mathcal{R}$ 如下。對著色 C_i，$C_j \in S$，其中 $1 \le i, j \le 16$，我們記 $C_i \mathcal{R} C_j$ 若存在一個排列 $\sigma \in G \ni \sigma^*(C_i) = C_j$。亦即，當 σ^* 作用在 S 上的 16 個圖案時，C_i 被轉換成 C_j。此關係 $\mathcal{R}$ 是一個等價關係，我們現在證明之。

a) (反身性質) 對所有 $C_i \in S$，其中 $1 \le i \le 16$，得 $C_i \mathcal{R} C_i$，因為 G 包含單位排列。[$\pi_0^*(C_i) = C_i$ 對所有 $1 \le i \le 16$。]

b) (對稱性質) 若 $C_i \mathcal{R} C_j$ 對 C_i，$C_j \in S$，則 $\sigma^*(C_i) = C_j$，對某些 $\sigma \in G$。G 是一個群，所以 $\sigma^{-1} \in G$，且我們發現 $(\sigma^*)^{-1} = (\sigma^{-1})^*$。(證明這個，對$\sigma \in G$ 的兩個選擇)。因此，$C_i = (\sigma^{-1})^*(C_j)$，且 $C_j \mathcal{R} C_i$。

c) (遞移性質) 令 C_i，C_j，$C_k \in S$ 滿足 $C_i \mathcal{R} C_j$ 且 $C_j \mathcal{R} C_k$，則 $C_j = \sigma^*(C_i)$ 且 $C_k = \tau^*(C_j)$，對某些 σ，$\tau \in G$。由 G 的封閉性，$\sigma\tau \in G$，且我們發現 $(\sigma\tau)^* = \sigma^*\tau^*$，其中 σ 被首先應用在 $\sigma\tau$ 且 σ^* 首先被應用在 $\sigma^*\tau^*$。(證明這個，對兩個明確的排列 σ，$\tau \in G$。) 則 $C_k = (\sigma\tau)^*(C_i)$ 且 $\mathcal{R}$ 是遞移的。[讀者可能已注意到 $C_k = \tau^*(C_j) = \tau^*(\sigma^*(C_i))$ 且感覺上我們應寫 $(\alpha\tau)^* = \tau^*\sigma^*$。再次，對我們在第 5 章首先定義的合成函數之記號有一改變。這裡我們以 $\sigma^*\tau^*$ 表 $(\sigma\tau)^*$ 且 σ^* 被先應用。]

因為 $\mathcal{R}$ 是 S 上的一等價關係，$\mathcal{R}$ 將 S 分割成等價類，即為圖 16.5 的等價類 $cl(1)$，$cl(2)$，…，$cl(6)$。因此，在這個群作用下，有 6 個非等價

圖案。所以在原先的 16 個著色中僅有 6 個是真的相異。

此例中所發生的被一般化如下。以一個圖案集 S，令 G 是作用在 S 的 (排列) 群。若 S 上的關係 $\mathcal{R}$ 被定義為 $x\ \mathcal{R}\ y$ 若 $\pi^*(x)=y$，對某些 $\pi \in G$, 則 $\mathcal{R}$ 是一個等價關係。

僅以紅色及白色圓盤來聯結牙籤，本例之答案已由圖 16.5 的結果決定了。然而，我們發展頗有一點數學威力的東西來回答問題。將 S 述為正方形頂點的 2-著色集，我們開始懷疑 2 的角色且開始尋找非等價類的個數，若圓盤有三個或更多個顏色。

此外，我們也許注意到 $f(r, w)=r^4+r^3w+2r^2w^2+rw^3+w^4$ 是 (兩變數的) 生成函數給 S 的非等價類圖案個數。這裡 r^iw^{4-i} 的係數，其中 $0 \le i \le 4$，產生有 i 個紅盤子及 $(4-i)$ 個白盤子的相異 2-著色個數。r^2w^2 的係數是 2，因為有兩個等價類 $c_1(3)$ 及 $c_1(4)$。最後，$f(1, 1)=6$，為等價類的個數。這個生成函數 $f(r, w)$ 被稱是圖案的**模型清單** (pattern inventory)。我們將更詳細的檢視它於下兩節。

現在我們將記下我們目前之結果的一個擴充版於下面定理裡。（此結果之證明被給在 C. L. Liu [17] 書的第 136-137 頁。）

定理 16.18 **Burnside 定理** (Burnside Theorem)。令 S 為一個圖案集，且 G 為作用在 S 上的排列有限群。S 被 G 作用的分割等價類個數是

$$\frac{1}{|G|}\sum_{\pi \in G}\psi(\pi^*),$$

其中 $\Psi(\pi^*)$ 是固定在 π^* 之下 S 中圖案的個數。

欲更加相信這個定理的有效性，我們首先檢視兩個例題，其中我們已經知道答案。

例題 16.29 在例題 16.28 中，我們發現 $\Psi(\pi_1^*)=2$，因為在 π_1^* 下僅 C_1 和 C_{16} 被固定，或不變的。然而，對 $r_3 \in G$，$\Psi(r_3^*)=8$，因為 C_1，C_2，C_4，C_{10}，C_{11}，C_{13}，C_{15}，及 C_{16} 在這個群作用下保持不變。同理，$\psi(\pi_2^*)=4$，$\psi(\pi_3^*)=2$，$\psi(\pi_0^*)=16$，$\psi(r_1^*)=\psi(r_2^*)=4$，且 $\psi(r_4^*)=8$。因 $|G|=8$，Burnside 定理告之等價類個數，或非等價圖案是 ψ

$$(1/8)(16+2+4+2+4+4+8+8)=(1/8)(48)=6,$$

為原先的答案。

例題 16.30

有多少種方法6 個人可被安排圍著一圓桌？若兩個安排被考慮等價，當之中一個可由另一個順時針旋轉 $i \cdot 60°$ 而得，其中 $0 \le i \le 5$。

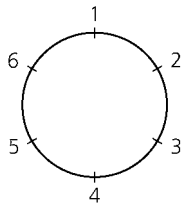


圖 16.7

這裡 6 位相異人被安置在圓桌的 6 張椅子，如圖 16.7 所示。我們的排列群 G 由順時針旋轉 $i \cdot 60°$ 的 π_i 所組成，其中 $0 \le i \le 5$。此處之鏡射沒有意義。這情況是 2-維的，因為我們僅可在平面旋轉圓 (代表圓桌) ；圓從未離開平面。可能的圖案總數是 6!，我們發現 $\Psi(\pi_0^*) = 6!$ 且 $\Psi(\pi_i^*) = 0$，對 $1 \le i \le 5$。(不可能移動不同的人且同時令他們停留在固定位置。)

因此，非等價座位安排的總數是

$$\left(\frac{1}{|G|}\right)\sum_{\sigma \in G}\psi(\sigma^*) = \left(\frac{1}{6}\right)(6! + 0 + 0 + 0 + 0 + 0) = 5!,$$

如我們在第 1 章例題 1.16 所發現的。

我們現在檢視一情況，其中這個定理的功能是明顯的。

例題 16.31

一正方形的所有頂點有多少種方法來 3-著色，若正方形可以三維來移動？

現在我們有例題 16.28 的牙籤，及紅色、白色和藍色盤子。考慮圖 16.6 的群，我們發現下面：

$\Psi(\pi_0^*) = 3^4$，因為單位排列固定可能圖案集 S 中的所有 81 個圖案。

$\Psi(\pi_1^*) = \Psi(\pi_3^*) = 3$，因為 π_1^*，π_3^* 各個僅將那些所有頂點均同色的圖案保留不變。

$\Psi(\pi_2^*) = 9$，因為 π_2^* 僅能將那些 (對角) 相對頂點有相同顏色的圖案固定。考慮一個像圖 16.8 所示的正方形。有三種選擇擺一個有色圓盤在頂點 1 及一個選擇給其配對的頂點 3。同樣的，有三種顏色選擇給頂點 2 及一個選擇給頂點 4。因此有 9 個圖案在 π_2^* 之下不變。

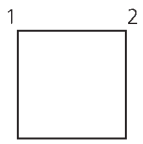


圖 16.8

$\Psi(r_1^*) = \Psi(r_2^*) = 9$。在 r_1^* 的情形，對圖 16.8 所示的正方形，我們有三種選擇來著色頂點 1 及頂點 2 各個，且我們必須將頂點 4 的顏色配對頂點 1 的顏色，且頂點 3 的顏色配對頂點 2 的顏色。

最後，$\Psi(r_3^*) = \Psi(r_4^*) = 27$。在 r_3^*，我們有九種選擇來著色在 2 和 4 的兩個頂點，及三種選擇給頂點 1。接著僅有一種選擇給頂點 3，因為我們必須配對頂點 1 的顏色。

由 Burnside 定理，非等價圖案的個數是

$$(1/8)(3^4 + 3 + 3^2 + 3 + 3^2 + 3^2 + 3^3 + 3^3) = 21.$$

習題 16.10

1. 考慮圖 16.5 所示的圖案。
   a) 求 π_2^*，π_3^*，r_2^*，及 r_4^*。
   b) 證明 $(\pi_1{}^1)^* = (\pi_1^*)^1$ 且 $(r_3{}^1)^* = (r_3^*)^1$。
   c) 證明 $(\pi_1 r_1)^* = \pi_1^* r_1^*$ 且 $(\pi_3 r_4)^* = \pi_3^* r_4^*$。
2. 將下面各個 S_7 的元素表為一個互斥循環的乘積。

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 7 & 1 & 5 & 3 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 2 & 1 & 7 & 4 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 7 & 5 & 4 & 6 \end{pmatrix}$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 1 & 3 & 6 & 5 \end{pmatrix}$$

3. a) 求習題 2 各個元素的階數。
   b) 利用其分解為一個互斥循環的乘積中各個循環的長度，敘述 S_n 中元素階數的一般結果。
4. a) 有多少種不同方法吾人可使用紅色及白色來著色一個等邊三角形的所有頂點，若這個三角形可在三維空間自由移動。
   b) 若藍色亦可使用，回答 (a)。
5. 對一正五邊形回答習題 4 的問題。
6. a) 有多少種方法以三種不同顏色來塗正方形的所有邊？
   b) 對一正五邊形回答 (a)。
7. 我們對稱的將四個有孔小珠珠串進一個圓形鐵絲來製做一個小孩手鐲。小珠珠的顏色是紅色、白色、藍色，及綠色，且每種顏色至少有 4 個小珠。(a) 依此法我們可做多少種不同的手鐲，若手鐲可被旋轉但不可鏡射？(b) 若手鐲可被旋轉及鏡射，回答 (a)。
8. 一根指揮棒以三種圓柱形色帶 (未必相異) 來裝飾，且每條色帶長度相同。
   a) 若有三種裝飾色可用，則可做多少種不同裝飾？若有四種顏色可用，則可做多少種不同裝飾？
   b) 對有 4 個圓柱形色帶的指揮棒回答 (a)。
   c) 對有 n 個圓柱形色帶的指揮棒回答 (a)。
   d) 若相鄰圓柱形色帶的顏色不同，回答 (a) 和 (b)。
9. 有多少種方法我們可 2-著色圖 16.9 所示的圖案的所有頂點若 (a) 它們可二維自由移動？(b) 它們可三維自由移動？

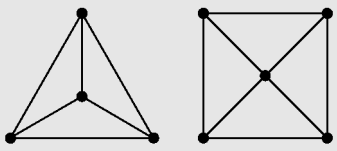


圖 16.9

10. 金字塔有正方形底座及四個等邊三角形的側面。若我們可以 (三維) 移動金字塔，有多少種非等價方法來塗它的五個

面，若我們有四種不同顏色可塗？有多少種方法可塗若底座的顏色必不同於三角形面的顏色？

11. a) 有多少種方法我們可使用紅色及藍色漆來漆一個 3×3 棋盤的格子？(棋盤的背面是黑色的。)
    b) 有多少種方法我們可以連接 (用膠水) 九個 1×1 透明且為紅色或為藍色的方格？(每個顏色有 9 個方格可用。)
12. 回答習題 11 給一個 4×4 的棋盤。[將 (b) 中的每個 "9" 取代為 "16"。]
13. 有多少種方法我們可使用黑色、褐色，及白色漆來漆騎術大會上的 7 匹 (相同的) 馬？
14. a) 令 S 是一個圖案集且 G 是作用在 S 上的一個排列群。若 $x \in S$，證明 $\{\pi \in G | \pi^*(x) = x\}$ 是 G 的一個子群 (稱之為 x 的**穩定子群** (stabilizer)。)
    b) 對圖 16.5 的圖案 C_7 及 C_{15} 各個分別求其在 (a) 的穩定子群。

16.11　循環指數

在應用 Burnside 定理時，我們已面臨計算 $\Psi(\pi^*)$ 對每個 $\pi \in G$，其中 G 是作用在圖案集 S 上的一個排列群。當可用的色數增加且圖案變得更複雜時，此類計算會有一點拖累。此外，似乎若我們可決定對一個圖案集 S 的 2-著色方法數，我們將能使用這情形的一些工作，來決定 3-著色、4-著色的方法數，且如此繼續。我們現在將發現有一點幫助，當我們回到例題 16.28 的解時。此次將更加注意每個 $\pi \in G$ 的表示式為一個互斥循環的乘積。我們的結果被整理於表 16.10 裡。

對 π_0，G 的單位元素，我們記 $\pi_0 = (1)(2)(3)(4)$，為一個四個互斥循環的乘積。我們將以 x_1^4 表示這個循環結構，其中 x_1 表一個長度為 1 的循環。x_1^4 這項被稱是 π_0 的**循環結構表示式** (cycle structure representation)。此處我們將 "互斥" 解讀為 "獨立" 意謂著不管甚麼顏色被用來塗一個循環上的所有頂點不必忍受另一個循環之所有頂點顏色的選擇。只要已知循環上的所有頂點有相同顏色，我們將發現圖案在 π_0^* 下是不變的。 (一般公認地，這似乎再次像過度的數學威力，只要當 π_0^* 固定正方形的所有 2-著色。) 此外，因我們可以紅色或白色來塗每個循環的所有頂點，我們有 2^4 個圖案，且我們發現 $(r+w)^4 = r^4 + 4r^3w + 6r^2w^2 + 4rw^3 + w^4$ 生成這 16 個圖案。例如，由 $6r^2w^2$ 這一項，我們發現有六個圖案有兩個紅色及兩個白色頂點，如在圖 16.5 的 $cl(3)$ 及 $cl(4)$ 兩類中所發現的。

轉到 π_1，我們發現 $\pi_1 = (1234)$，一個長度為 4 的循環。這個循環結

表 16.10

剛體運動 π (G的元素)	在 π^* 下不變的 S 中之圖案	π的循環結構表示式	在 π^* 下不變的圖案清單
$\pi_0 = (1)(2)(3)(4)$	2^4: S 的所有圖案	x_1^4	$(r+w)^4 = r^4 + 4r^3w + 6r^2w^2 + 4rw^3 + w^4$
$\pi_1 = (1234)$	2: C_1, C_{16}	x_4	$r^4 + w^4 = r^4 + w^4$
$\pi_2 = (13)(24)$	2^2: C_1, C_{10}, C_{11}, C_{16}	x_2^2	$(r^2+w^2)^2 = r^4 + 2r^2w^2 + w^4$
$\pi_3 = (1432)$	2: C_1, C_{16}	x_4	$r^4 + w^4 = r^4 + w^4$
$r_1 = (14)(23)$	2^2: C_1, C_7, C_9, C_{16}	x_2^2	$(r^2+w^2)^2 = r^4 + 2r^2w^2 + w^4$
$r_2 = (12)(34)$	2^2: C_1, C_6, C_8, C_{16}	x_2^2	$(r^2+w^2)^2 = r^4 + 2r^2w^2 + w^4$
$r_3 = (13)(2)(4)$	2^3: C_1, C_2, C_4, C_{10}, C_{11}, C_{12}, C_{15}, C_{16}	$x_2x_1^2$	$(r^2+w^2)(r+w)^2 = r^4 + 2r^3w + 2r^2w^2 + 2rw^3 + w^4$
$r_4 = (1)(24)(3)$	2^3: C_1, C_3, C_5, C_{10}, C_{11}, C_{12}, C_{14}, C_{16}	$x_2x_1^2$	$(r^2+w^2)(r+w)^2 = r^4 + 2r^3w + 2r^2w^2 + 2rw^3 + w^4$
	$P_G(x_1, x_2, x_3, x_4) = \frac{1}{8}(x_1^4 + 2x_4 + 3x_2^2 + 2x_2x_1^2)$		完整清單 $= 8r^4 + 8r^3w + 16r^2w^2 + 8rw^3 + 8w^4$

構被表為 x_4，且此處僅有兩個不變的圖案。π_1 的循環結構僅有一個循環的事實告訴我們一個圖案要在 π_1^* 下不變，這個循環上的每個頂點必被塗同一顏色。以有兩種顏色來選，僅有兩種可能圖案，即 C_1 和 C_{16}。此時 r^4+w^4 項產生這些圖案。

以 r_1 繼續，我們有 r_1=(14)(23)，兩個長度為 2 的互斥循環乘積；x_2^2 項表示這個循環結構。一個圖案要在 r_1^* 下不變，在 2 和 3 的頂點必為同色；亦即，我們有兩個選擇來著色 (23) 的所有頂點。我們亦有兩個選擇來著色 (14) 的所有頂點。因此，我們得到 2^2 個不變圖案：$C_1(r^4)$，$C_7(r^2w^2)$，$C_9(r^2w^2)$，及 $C_{16}(w^4)$。[$(r^2+w^2)^2 = r^4+2r^2w^2+w^4$。]

最後，在 r_3=(13)(2)(4) 的情形，我們發現 $x^2x_1^2$ 表示其被分解為一個長度為 2 的循環及兩個長度為 1 的循環。在 1 和 3 的頂點必被塗同一顏色，若圖案要在 r_3^* 下不變。以三個循環及每個循環有兩種顏色選擇，我們發現 2^3 個不變圖案。它們是 $C_1(r^4)$，$C_2(r^3w)$，$C_4(r^3w)$，$C_{10}(r^2w^2)$，$C_{11}(r^2w^2)$，$C_{13}(rw^3)$，$C_{15}(rw^3)$，及 $C_{16}(w^4)$。這些圖案以 $(r^2+w^2)(r+w)^2$ 來生成，因為當我們考慮循環 (13) 時，我們有兩種選擇：兩個頂點均為紅色 (r^2) 或兩個頂點均為白色 (w^2)。此給我們 r^2+w^2。對長度為 1 的兩個循環中的每個單一頂點，$r+w$ 提供選擇給每個循環，$(r+w)^2$ 提供選擇給兩個

循環。以顏色選擇的獨立性，當我們由一個循環走到另一個循環，$(r^2+w^2)(r+w)^2$ 產生 2^3 個在 r_3^* 下不變的圖案。

同理可提供表16.10 的資訊給排列 π_2，π_3，r_2，及 r_4。

目前我們看到決定在 π^* 下不變的圖案個數，對 $\pi \in G$，是依據 π 的循環結構。在每個循環間相同顏色必被使用，但顏色可由兩個或更多個可用的選擇來選擇。對 r_1，我們有兩個長度為 2 的循環及 2^2 個圖案。若有三種顏色可用，不變的圖案個數將是 3^2。對 m 種顏色，則個數為 m^2。加總這些項給所有循環結構得 $\sum_{\pi\in G}\psi(\pi^*)$。

我們現在想擺更多的強調在循環結構上，所以我們定義**循環指數** (cycle index)，P_G，給 (排列) 群 G，為

$$P_G(x_1, x_2, x_3, x_4) = \frac{1}{|G|}\sum_{\pi\in G}(\pi\text{的循環結構表示式})$$

在本例中，

$$P_G(x_1, x_2, x_3, x_4) = (1/8)(x_1^4 + 2x_4 + 3x_2^2 + 2x_2x_1^2).$$

當每個 x_1，x_2，x_3，x_4 被取代為 2 時，我們發現非等價 2-著色的個數是

$$P_G(2, 2, 2, 2) = (1/8)(2^4 + 2(2) + 3(2^2) + 2(2)(2^2)) = 6.$$

我們將目前的發現整理於下面結果。

定理 16.19

令 S 為一個圖案集，且排列群 G 作用在 S 上。[G 是 S_n 的子群，S_n 是 $\{1, 2, 3, \cdots, n\}$ 的所有排列所成的群，且 G 的循環指數 $P_G(x_1, x_2, \cdots, x_n)$ 是

$$(1/|G|)\sum_{\pi\in G}(\pi\text{的循環結構表示式})。]$$

則 S 的非等價 m-著色個數是 $P_G(m, m, m, \cdots, m)$。

我們以使用這個定理的例題來結束本節。

例題 16.32

有多少種不同方法我們可 4-著色一個正六邊形的所有頂點？這個正六邊形可在空中自由移動。

一個正六邊形有 12 個剛體運動：(a) 旋轉 0°，60°，120°，180°，240°，及 300° 的六個順時針旋轉；(b) 以經過相對頂點的對角線所做的三個鏡射；及 (c) 以經過對邊中點的直線所做的三個鏡射。

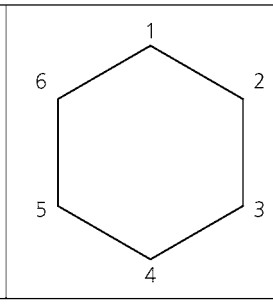
(1)	(1)(2)(3)(4)(5)(6)	x_1^6		(7)	(1)(26)(35)(4)	$x_1^2x_2^2$
(2)	(123456)	x_6		(8)	(13)(46)(2)(5)	$x_1^2x_2^2$
(3)	(135)(246)	x_3^2		(9)	(15)(24)(3)(6)	$x_1^2x_2^2$
(4)	(14)(25)(36)	x_2^3		(10)	(12)(36)(45)	x_2^3
(5)	(153)(264)	x_3^2		(11)	(14)(23)(56)	x_2^3
(6)	(165432)	x_6		(12)	(16)(25)(34)	x_2^3

圖 16.10

在圖 16.10 裡，我們已列出每個群元素為一個互斥循環的乘積，及其循環結構表示式。此處

$$P_G(x_1, x_2, x_3, x_4, x_5, x_6) = (1/12)(x_1^6 + 2x_6 + 2x_3^2 + 4x_2^3 + 3x_1^2x_2^2),$$

且有

$$P_G(4, 4, 4, 4, 4, 4) = (1/12)(4^6 + 2(4) + 2(4^2) + 4(4^3) + 3(4^2)(4^2)) = 430$$

個非等價的正六邊形的 4-著色。(注意：甚至 x_4 和 x_5 不出現在循環結構表示式裡，我們可將這些變數列在 P_G 的自變數中。)

習題 16.11

1. 有多少種方法我們可 5-著色一個正方形的所有頂點？(a) 此正方形可二維自由移動。(b) 此正方形可三維自由移動。
2. 對一正五邊形回答習題 1。
3. 求圖 16.11 所示的圖案之所有頂點的非等價 4-著色個數，當它們 (a) 可二維自由移動；(b) 可三維自由移動。
4. a) 有多少種方法我們可 3-著色一個可在空中自由移動的正六邊形的所有頂點？
   b) 給一個組合理論證明對所有 $m \in \mathbf{Z}^+$，$(m^6 + 2m + 2m^2 + 4m^3 + 3m^4)$ 可被 12 整除。

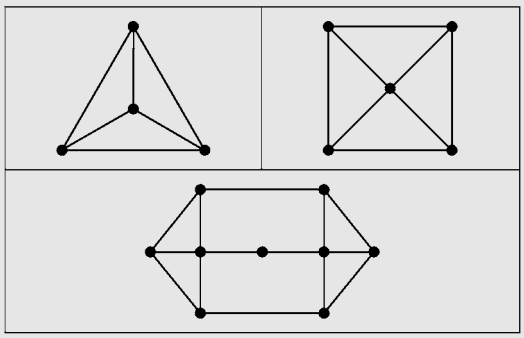


圖 16.11

5. a) 有多少種方法我們可 5-著色一個可二維自由移動的正六邊形的所有頂點？
   b) 若六邊形可三維自由移動，回答 (a)。

c) 找兩個 5-著色使其和 (b) 等價但和 (a) 不同。

6. 有多少種不同方法我們可 3-著色圖 16.11 所示的圖案的所有邊，若它們可 (a) 二維自由移動；(b) 三維自由移動？
7. a) 有多少種不同方法我們可 3-著色一個可三維自由移動的正方形的所有邊？
   b) 有多少種不同方法我們可 3-著色此一正方形的所有頂點及所有邊？
   c) 給一個可三維移動的正方形，令 k，m，及 n 分別表我們可 3-著色其頂點 (單獨)，其邊 (單獨)，及頂點和邊，則 $n=km$ 嗎？(給一個幾何解釋。)

16.12　模型清單：Polya 枚舉法

最後一節，我們回到例題 16.28 且繼續其在 16.11 節所做的分析，此刻我們將介紹模型清單及它是如何由循環指數導出的。

對 $\pi_0 \in G$，每個 S 中的圖案是不變的。π_0 的循環結構 (表示式) 被給為 x_1^4，其中對每個長度為 1 的各個循環，我們有一個選擇來著色該循環頂點為紅色 (r) 或白色 (w)。使用＋表**互斥或** (exclusive or)，我們記 $r+w$ 表該頂點 (長度為 1 的循環) 的兩個選擇。以 4 個此類循環，$(r+w)^4$ 生成 16 個圖案的模型。

在 $\pi_1=(1234)$ 的情形，x_4 表循環結構，且所有 4 個頂點必同色，因為圖案在 π_1^* 下保持不變。因此，我們有 4 個頂點均為紅色或 4 個頂點均為白色，且我們代數式的將這個表為 r^4+w^4。

此刻我們注意到，對各個我們已考慮的排列，被用來生成在某個排列下固定的模型的表示式之因式個數等於該排列之循環結構 (表示式) 的因式個數。這僅是一種巧合嗎？

現在以 $r_1=(14)(23)$ 繼續，其循環結構是 x_2^2。對循環 (14)，我們必須對頂點 1 及 4 同時著紅色或白色。這些選擇被表為 r^2+w^2。因為有兩個長度為 2 的此類循環。我們發現 $(r^2+w^2)^2$ 將生成固定在 r_1^* 下的 S 圖案的模型。再次地，循環結構中的因式個數等於用生成模型的相對應項之因式個數。

最後，對 $r_3=(13)(2)(4)$，循環結構是 $x_2x_1^2=x_1^2x_2$。對循環 (2) 及 (4) 的各個，$r+w$ 表示選擇給這些頂點的各個，所以 $(r+w)^2$ 說明這對頂點的所有四著色。循環 (13) 說明頂點 1 和 3 必同色，r^2+w^2 說明這兩個可能。因此，$(r+w)^2(r^2+w^2)$ 生成 S 中固定在 r_3^* 下的圖案模型，且我們在兩個

循環結構中發現三個因式及乘積 $(r+w)^2(r^2+w^2)$。但這裡甚至更多曙光出現。

看看循環結構中的所有項，我們看到，對 $1 \le i \le n$，循環結構中的因式 x_i 對應用來生成模型的表示式中的 r^i+w^i 這一項。

以 π_2，π_3，r_2，及 r_4 的循環結構繼續，我們發現將 $P_G(x_1, x_2, x_3, x_4)$ 中的各個 x_i 取代為 r^i+w^i，可得**模型清單** (pattern inventory)，對 $1 \le i \le 4$。因此，

$$P_G(r+w, r^2+w^2, r^3+w^3, r^4+w^4) = r^4+r^3w+2r^2w^2+rw^3+w^4.$$

(此結果是表 16.10 所列的完整清單的第 (1/8) 個。)

若我們有三種顏色 (紅、白，及藍)，x_i 的替代值將為 $r^i+w^i+b^i$，其中 $1 \le i \le 4$。

我們將這些結果一般化於下面定理。

定理 16.20

Polya 枚舉法 (Polya's Method of Enumeration)。令 S 為一個圖案集，且被一個排列群 G 作用在其上，其中 G 是 S_n 的子群，且 G 有循環指數 $P_G(x_1, x_2, \cdots, x_n)$。則 S 的非等價 m-著色模型清單被給為

$$P_G\left(\sum_{i=1}^{m} c_i, \sum_{i=1}^{m} c_i^2, \ldots, \sum_{i=1}^{m} c_i^n\right),$$

其中 $c_1, c_2, \cdots, c_m$ 表有 m 個顏色可用。

在應用定理 16.20 之前，一個重點在此應被再敘述——即模型清單是生成函數的另一個例子。有了該觀點，我們現在應用這個定理於下面例題裡。

例題 16.33

一個小孩的手鐲係將 3 個小珠——紅色、白色，及藍色串在一個圓形的鐵線而成的。手鐲被認為是等價的，若一個可由另一個經由 (平面) 旋轉獲得。求模型清單給這些手鐲。

此處 G 是一個等邊三角形的旋轉群，所以 $G=\{(1)(2)(3), (123), (132)\}$，其中 1，2，3 表三角形的三個頂點。則 $P_G(x_1, x_2, x_3)=(1/3)\cdot(x_1^3+2x_3)$，且模型清單是 $(1/3)[(r+w+b)^3+2(r^3+w^3+b^3)]=(1/3)[3r^3+3r^2w+3r^2b+3rw^2+6rwb+3rb^2+3w^3+3w^2b+3wb^2+3b^3]=r^3+r^2w+r^2b+rw^2+2rwb+rb^2+w^3+w^2b+wb^2+b^3$。我們將這個結果解讀如下：

1) 除 $2rwb$ 外，每個被加項的係數是 1，因為僅有一個該型態的 (不同) 手鐲。亦即，有一個含三個小紅珠 (對 r^3) 的手鐲，一個含兩個小紅珠及一個小白珠 (對 r^2w) 的手鐲，且如此繼續對其它七個具係數 1 的被加項。
2) 被加項 $2rwb$ 有係數 2，因為有兩個具一小紅珠、一小白珠，及一小藍珠的非等價手鐲，如圖 16.12 所示。

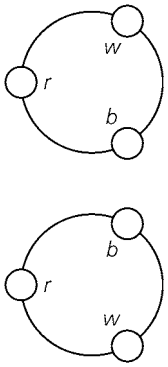


圖 16.12

若手鐲亦可被鏡射，則 G 變為 {(1)(2)(3), (123), (132), (1)(23), (2)(13), (3)(12)}，且這裡的模型清單和上面的一個相同，但有一個例外。這裡我們有 rwb 代替 $2rwb$，因為圖 16.12 的非等價 (對旋轉) 模型變為等價當鏡射被允許時。

例題 16.34

考慮例題 16.28 中圖案的 3-著色，若三個顏色為紅色、白色，及藍色，多少個非等價圖案恰有兩個紅色頂點？

給 $P_G(x_1, x_2, x_3, x_4)=(1/8)(x_1^4+2x_4+3x_2^2+2x_2x_1^2)$，答案是 r^2w^2，r^2b^2，及 r^2wb 在 $(1/8)[(r+w+b)^4+2(r^4+w^4+b^4)+3(r^2+w^2+b^2)^2+2(r^2+w^2+b^2)(r+w+b)^2]$ 中的係數和。

在 $(r+w+b)^4$ 中，我們發現 $6r^2w^2+6r^2b^2+12r^2wb$。對 $3(r^2+w^2+b^2)^2$，我們對 $6r^2w^2+6r^2b^2$ 項有興趣，而 $4r^2w^2+4r^2b^2+4r^2bw$ 出現於 $2(r^2+w^2+b^2)(r+w+b)^2$ 中。

則 $(1/8)[6r^2w^2+6r^2b^2+12r^2wb+6r^2w^2+6r^2b^2+4r^2w^2+4r^2b^2+4r^2bw]=2r^2w^2+2r^2b^2+2r^2bw$，為恰含兩個紅色頂點的六個非等價圖案的清單。

下一個例題處理模型清單給正方體所有頂點的 2-著色。 (顏色為紅色及白色)

例題 16.35

對圖 16.13 的正方體，我們發現它的剛體運動群由下面組成。

1) 含循環結構 x_1^8 的單位變換。
2) 對一個過兩個對面中心的軸做 90°，180°，及 270° 的旋轉：由圖 16.13(a) 我們有

90° 旋轉：(1234)(5678)	循環結構：x_4^2
180° 旋轉：(13)(24)(57)(68)	循環結構：x_2^4
270° 旋轉：(1432)(5876)	循環結構：x_4^2

因為有兩對其它對面，這九個旋轉說明 $3x_2^4+6x_4^2$ 項於循環指數裡。

3) 對一個過兩個對邊中點的軸做 180° 旋轉：如圖 16.13(b)，我們有排列 (17)(28)(34)(56)，其循環結構是 x_2^4。有六對對邊，這些旋轉貢獻 $6x_2^4$ 項給循環指數。

4) 對一個通過兩對角點的軸做 120° 及 240° 的旋轉：由圖 (c) 我們有

120° 旋轉：(168)(274)(3)(5)　　循環結構：$x_1^2x_3^2$
240° 旋轉：(186)(247)(3)(5)　　循環結構：$x_1^2x_3^2$

這裡有四個這樣的頂點對，且這些給循環指數中的 $8x_1^2x_3^2$。

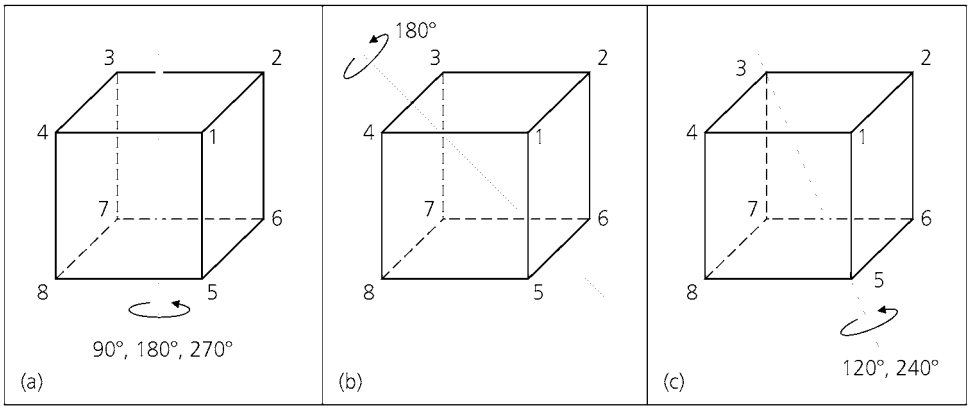


圖 16.13

因此，$P_G(x_1, x_2, \cdots, x_8) = (1/24)(x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2)$，且這些圖案的模型清單被以生成函數

$$f(r, w) = (1/24)[(r+w)^8 + 9(r^2+w^2)^4 + 6(r^4+w^4)^2 + 8(r+w)^2(r^3+w^3)^2]$$
$$= r^8 + r^7w + 3r^6w^2 + 3r^5w^3 + 7r^4w^4 + 3r^3w^5 + 3r^2w^6 + rw^7 + w^8.$$

給之，將 r 和 w 取代為 1，我們發現這裡有 23 個非等價關係。

因為 Polya 枚舉法首先被發展來計數有機化合物的異構體，我們以處理某類有機化合物的應用來結束本節。這是基於 C. L. Liu 的一個例題 (參見參考資料 [17] 的 152-154。)

例題 16.36

這裡我們考慮圖 16.14 所示的有機分子型，其中 C 是一個碳原子且 X 表下面分子的任一個：Br (溴)，H (氫)，CH_3 (甲基)，或 C_2H_5 (乙基)。例如，若每個 X 被取代為 H，則得化合物 CH_4 (甲烷)。圖 16.14 將不允許誤導我們。這些有機化合物的結構是三維的。因此，我們轉到正四面體來模

擬這個結構。我們將把碳原子擺在正四面體的中心，並將給 X 的選擇擺在頂點 1，2，3 及 4，如圖 16.15 所示。

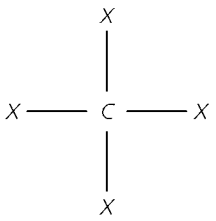


圖 16.14

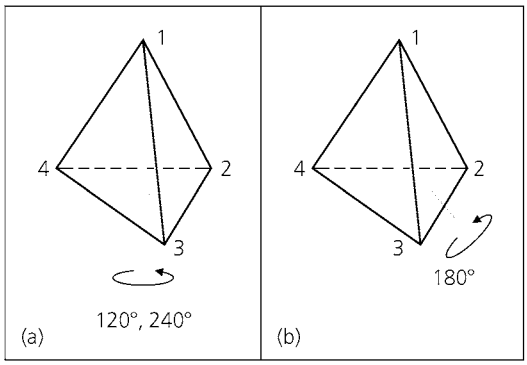


圖 16.15

作用在這些圖案的群 G 被如下給之：

1) 含循環結構 x_1^4 的單位變換 (1)(2)(3)(4)。
2) 對一個過一頂點及對面之中心的軸做 120° 或 240° 的旋轉。如圖 16.15(a) 所示，我們有

   120° 旋轉：(1)(243) 具循環結構 x_1x_3
   240° 旋轉：(1)(234) 具循環結構 x_1x_3

   由於對稱的關係，還有三組頂點及對面，所以這些剛體運動說明 $P_G(x_1, x_2, x_3, x_4)$ 中的 $8x_1x_3$ 項。
3) 對一個通過兩對邊中點的軸做 180° 旋轉：圖 (b) 所示的情形被以排列 (14)(23) 給之，其循環結構是 x_2^2。有三對對邊，我們得 $P_G(x_1, x_2, x_3, x_4)$ 的 $3x_2^2$ 項。

因此，$P_G(x_1, x_2, x_3, x_4) = (1/12)[x_1^4 + 8x_1x_3 + 3x_2^2]$ 且 $P_G(4, 4, 4, 4) = (1/12) \cdot [4^4 + 8(4^2) + 3(4^2)] = 36$，所以有 36 個不同的有機化合物可依此法得到。

最後，若我們想知道這些化合物中有多少個恰有兩個溴原子，我們令 w，x，y，及 z 分別表“顏色” Br，H，CH_3，及 C_2H_5，且求 w^2x^2，w^2y^2，w^2z^2，w^2xy，w^2xz, 及 w^2yz 於模型清單

$$(1/12)[(w + x + y + z)^4 + 8(w + x + y + z)(w^3 + x^3 + y^3 + z^3) + 3(w^2 + x^2 + y^2 + z^2)^2].$$

中的係數和。

對 $(w+x+y+z)^4$ 有關的項是 $6w^2x^2+6w^2y^2+6w^2z^2+12w^2xy+12w^2xz+12w^2yz$。模型清單的中間加項不出現在渴望的圖案中的任一個，而在 $3(w^2+x^2+y^2+z^2)^2$ 中，我們發現 $6w^2x^2+6w^2y^2+6w^2z^2$。

因此，給恰含兩個溴原子的化合物之模型清單是

$$(1/12)[12w^2x^2+12w^2y^2+12w^2z^2+12w^2xy+12w^2xz+12w^2yz]$$

且有 6 個此類的有機化合物。

習題 16.12

1. a) 求模型清單給一正方形的所有邊的 2-著色，其中正方形 (i) 可二維自由移動；(ii) 可三維自由移動。(令顏色為紅色及白色。)
   b) 對 3-著色回答 (a)，其中顏色為紅色、白色，及藍色。
2. 若一正五邊形可在空中自由移動，且我們可以紅色、白色，及藍色漆來塗其頂點，有多少個非等價圖案恰有三個紅色頂點？有多少個有兩個紅色、一個白色，及兩個藍色頂點？
3. 假設在例題 16.35 中，我們 2-著色正方體的所有的面，此正方體可在空中自由移動。
   a) 這個情形有多少個不同的 2-著色。
   b) 若可用的顏色是紅色及白色，求其模型清單。
   c) 有多少個非等價著色有三個紅色及三個白色面？
4. 對例題 16.36 的有機化合物，有多少個化合物至少有一個溴原子？有多少個化合物恰有三個氫原子？
5. 找模型清單給圖 16.11 的圖案之頂點的 2-著色，當它們可在空中自由移動時。(令顏色為綠色及金色。)
6. a) 有多少種方法可以黑色、褐色及白色漆來塗騎術大會的七匹 (相同的) 馬，使得有三匹黑色、兩匹褐色，及兩匹白色馬？
   b) 有多少種方法可使黑色馬及褐色馬的個數相同？
   c) 給一個組合理論證明對所有 $n \in \mathbf{Z}^+$，n^7+6n 被 7 整除。
7. a) 有多少個方法我們可使用紅色及白色來漆一個 2×4 棋盤的八個方格？(棋盤的背面是黑棋盤。)
   b) 找模型清單給 (a) 的著色。
   c) (a) 中有多少種著色有四個紅色及四個白色方格？多少種著色有六個紅色及兩個白色方格？
8. a) 有多少個方法我們可使用黑色及金色來給圖 16.16 所示的紙風車的八個區域 2-著色，若每個區域的背面是灰色？
   b) 使用黑色、金色，及藍色漆來塗所有區域，對這可能的 3-著色，回答 (a)。

c) 對 (b) 中的著色，有多少個有四個黑色、兩個金色，及兩個藍色區域？

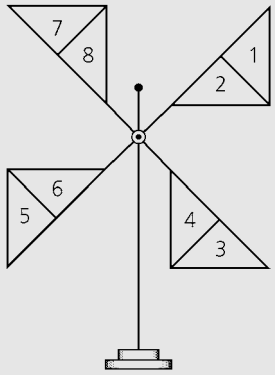


圖 16.16

9. 令 m，$n \in \mathbf{Z}^+$且 $n \geq 3$。有多少個被加項出現在給正 n 邊形所有頂點之 m-著色的模型清單裡？

16.13　總結及歷史回顧

雖然變換群的觀念逐漸發展於幾何的研究裡，但群概念發展的主要推動力來自多項式方程的研究。

解二次方程的方法出自古希臘。接著在 16 世紀，進展至解三次及四次多項式方程，其中之係數為有理數。繼續至五次及更高次的多項式方程式，Leonhard Euler (1707-1783) 及 Joseph-Louis Lagrange (1736-1813) 企圖解一般的五次方程。Lagrange 瞭解多項式方程的次數 n 和排列群 S_n 間必有一個聯結。然而，最後是 Niels Henrik Abel (1802-1829) 證明了不可能有公式僅使用加法、減法、乘法、除法，及開根號來解一般的五次方程式。在同一時期，具有理係數次數 ≥ 5 的多項式可以根式來解的充分必要條件被探討且被優秀的法國數學家 Evariste Galois (1811-1832) 解出來。因為 Galois 的作品同時使用群和體的結構，我們將在第 17 章的總結裡多說說他。

檢視 J. Stillwell [28] 的第 278-280 頁，我們發現群概念，且事實上“群”這個字首先出現於 Galois 於 1831 年出版的作品 *Mémoire sur les conditions de résolubilité des équations par radicaux* 裡。聯想的，群單位元素及反元素是 Galois 的假設之結果，因為他僅處理一個有限集合的排列群，且他的群定義僅需封閉性。第一位發現需敘述結合性給群元素的是 Arthur Cayley (1821-1895) (於 1854 年，在他的論文 *On the Theory of*

Niels Henrik Abel (1802-1829)

Groups, as Depending on the Symbolic Equation $\theta^n = 1$ 裡)。第一個真正把反元素併入群定義的敘述出於 1883 年由 Walther Franz Anton von Dyck (1856-1934) 的文章 *Gruppentheoretischen Studien II* 裡。

傍集的概念，我們介紹於 16.3 節，亦是由 Evariste Galois (在 1832 年) 所發展的。真正的名詞係由 George Abram Miller (1863-1951) (於 1910 年) 所鑄造出來的。

隨著 Galois 的成就，群理論影響許多數學領域。例如，在 19 世紀末，德國數學家 Felix Klein (1849-1929)，在已成名的 *Erlanger Programm* 裡，企圖依據保有幾何性質不變的變換群來編寫所有存在的幾何。

其它許多數學家，諸如 Augustin-Louis Cauchy (1789-1857)，Arthur Cayley (1821-1895)，Ludwig Sylow (1832-1918)，Richard Dedekind (1831-1916)，及 Leopold Kronecker (1823-1891)，貢獻某種型態的群的更進一步發展。然而，直到 1900 年，定義條件的表列才被給一般抽象的群。

在 20 世紀間，有許多研究企圖來解悉有限群的結構，對有限交換群，大家都知道任何此類群等價於階數為質冪次方的循環群的直積。然而，有限非交換群則變為相當的複雜。以 Galois 的作品開始，吾人發現特別小心來注意一個所謂的正規子群之子群型。對任意群 G， (G 的) 子群 H 被稱是**正規的** (normal) 若對所有 $g \in G$ 及所有 $h \in H$，我們有 $ghg^{-1} \in H$。在一個交換群裡，每個子群均是正規的，但對非交換群則不是。在每個群 G 裡，$\{e\}$ 和 G 均是正規子群，但若 G 沒有其它正規子群，則稱它是**單純的** (simple)。在過去六十年間，數學家已搜尋且決定出所有的有限單純群，並檢視它們在所有有限群結構中的角色。有限單純群分類的主

要推動者中有 Walter Feit，John Thompson，Dani Gorenstein，Michael Aschbacher，及 Robert Griess, Jr 等幾位教授。欲知更多歷史及這個有紀念的研究之影響，讀者可參考 J. A. Gallian [5]，A. Gardin [7]，M. Gardner [9]，R. Silvestri [27]，尤其是 D. Gorenstein [13] 的文章。

有許多教科書吾人可進一步來學習群的理論。在導引的層次，J. A. Gallian [6] 及 V. H. Larney [16] 的書提供高於本章所介紹的進一步教材。I. N. Herstein [15] 是一部好的資料書且包含 Galois 理論的材料。

更多有關 16.4 節的 RSA 公開-鍵值的密碼系統可被發現於參考資料中的 T. H. Barr [2]，P. Garrett [10]，及 W. Trappe 和 L. C. Washington [31] 裡。這個系統的早先描述被給於 M. Gardner [8] 的文章裡，其中訊息係使用，模 n，一個 64-位元質數及一個 65-位元質數的乘積來編碼。G. Taubes [30] 文章敘述 Arjen Lenstra，Paul Leyland，Michael Graff，及 Derek Atins，和 600 位自願者分解 n 的努力。

代數編碼理論的源頭可追朔到 1941 年，Claude Elwood Shannon 開始他在傳送方面問題的探討。這些問題由於戰爭的需要而快速產生。他的研究得到許多新的概念及原理且在 1948 年出版於學報文章裡 [26]。由於這個研究，Shannon 被公認為是資訊理論的開創者。在這個出版後，M. J. E. Golay [11] 及 R. W. Hamming [14] 的結果馬上跟著來，給進一步的衝力來研究這個領域。在 F. J. MacWilliams 及 N. J. A. Sloane [18] 書的第二冊末之參考文獻所列的 1478 個參考資料傳達這個領域在 1950 及 1975 年期間這個活動的一些概念。

我們的編碼理論教材是跟著 L. L. Dornhoff 及 F. E. Hohn[4] 的第 5 章之材料。E. F. Assmus, Jr.，和 J. D. Key [1]，S. W. Golomb，R. A. Scholtz，和 R. E. Peile [12]，V. Pless [20]，及 S. Roman [24] 等書以適合中等層次的方式提供新的主題材料。編碼方面更進一步的研究可被發現於 F. J. MacWilliams 和 M. J. A. Sloane [18]，S. Roman [25]，及 A. P. Street 和 W. D. Wallis [29] 的書裡。使用鴿洞原理於編碼理論的有趣應用被給於 [29] 的第 11 章。

在本章的 10，11，及 12 節裡，我們提出一個枚舉技巧，它的發展要歸功於匈牙利數學家 George Polya (1887-1985)。他的文章 [21] 提供基本技巧來計數化學異構體、圖論，及樹形的等價類。 (對某些範圍，這個研究中的概念係由 J. H. Redfield [23] 事前先處理的。) 因為這些技巧已被發現付諸如布林函數的電子真實感領域方面的計數問題是無價的。Polya 基本定理首先被一般化於 N. G. DeBruijn [3] 的文章裡，且這些概念的擴充可被發現於文獻裡。R. C. Read [22] 的文章敘述 Polya 定理在組合分析上

的巨大影響。(包含這篇文章的學報亦包含其它許多處理 George Polya 一生及作品的文章。)

我們的這個題裁的教材是跟隨 A. Tucker [32] 文章所給的材料。這個方法一個更嚴密的呈現可被發現於 C. L. Liu [17] 的第 5 章。

在處理 Burnside 定理時，我們有另一個不正確歸屬的例子。當我們學習 P. M. Neumann [19] 的文章時，這個結果出現在 Georg Frobenius (1848-1917) 於 1887 年發表的一篇論文裡，也出現在 Cauchy 1845 年的一些研究裡。

參考資料

1. Assmus, E. F., Jr., and Key, J. D. *Designs and Their Codes*. New York: Cambridge University Press, 1992.
2. Barr, Thomas H. *Invitation to Cryptology*. Upper Saddle River, N. J.: Prentice-Hall, 2002.
3. DeBruijn, Nicolaas Govert. "Polya's Theory of Counting." Chapter 5 in *Applied Combinatorial Mathematics*, ed. by Edwin F. Beckenbach. New York: Wiley, 1964.
4. Dornhoff, Larry L., and Hohn, Franz E. *Applied Modern Algebra*. New York: Macmillan, 1978.
5. Gallian, Joseph A. "The Search for Finite Simple Groups." *Mathematics Magazine* 49, 1976, pp. 163–179.
6. Gallian, Joseph A. *Contemporary Abstract Algebra*, 5th ed. Boston, Mass.: Houghton Mifflin, 2002.
7. Gardiner, Anthony. "Groups of Monsters." *New Scientist*, April 5, 1979, p. 34.
8. Gardner, Martin. "A New Kind of Cipher That Would Take Millions of Years to Break." *Scientific American* (August 1977): pp. 120–124.
9. Gardner, Martin. "The Capture of the Monster: A Mathematical Group with a Ridiculous Number of Elements." *Scientific American* 242 (6), 1980, pp. 20–32.
10. Garrett, Paul. *Making, Breaking Codes: An Introduction to Cryptology.* Upper Saddle River, N. J.: Prentice-Hall, 2001.
11. Golay, Marcel J. E. "Notes on Digital Coding." *Proceedings of the IRE* 37, 1949, p. 657.
12. Golomb, Solomon W., Scholtz, Robert A., and Peile, Robert E. *Basic Concepts in Information Theory and Coding*. New York: Plenum, 1994.
13. Gorenstein, Daniel. "The Enormous Theorem." *Scientific American* 253 (6), 1985, pp. 104–115.
14. Hamming, Richard Wesley. "Error Detecting and Error Correcting Codes." *Bell System Technical Journal* 29, 1950, pp. 147–160.
15. Herstein, Israel Nathan. *Topics in Algebra*, 2nd ed. Lexington, Mass.: Xerox College Publishing, 1975.
16. Larney, Violet H. *Abstract Algebra: A First Course*. Boston: Prindle, Weber & Schmidt, 1975.
17. Liu, C. L. *Introduction to Combinatorial Mathematics*. New York: McGraw-Hill, 1968.
18. MacWilliams, F. Jessie, and Sloane, Neil J. A. *The Theory of Error-Correcting Codes*, Volumes I and II. Amsterdam: North-Holland, 1977.
19. Neumann, Peter M. "A Lemma That Is Not Burnside's." *The Mathematical Scientist*, Vol. 4, 1979, pp. 133–141.
20. Pless, Vera. *Introduction to the Theory of Error-Correcting Codes*, 2nd ed. New York: Wiley, 1989.
21. Polya, George. "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemishe Verbindungen." *Acta Mathematica* 68, 1937, pp. 145–254.
22. Read, R. C. "Polya's Theorem and Its Progeny." *Mathematics Magazine* 60, 1987, pp. 275–282.

23. Redfield, J. Howard. "The Theory of Group Reduced Distributions." *American Journal of Mathematics* 49, 1927, pp. 433–455.
24. Roman, Steven. *Introduction to Coding and Information Theory*. New York: Springer-Verlag, 1997.
25. Roman, Steven. *Coding and Information Theory*. New York: Springer-Verlag, 1992.
26. Shannon, Claude E. "The Mathematical Theory of Communication." *Bell System Technical Journal* 27, 1948, pp. 379–423, 623–656. Reprinted in C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1949).
27. Silvestri, Richard. "Simple Groups of Finite Order." *Archive for the History of Exact Sciences* 20, 1979, pp. 313–356.
28. Stillwell, John. *Mathematics and Its History*. New York: Springer-Verlag, 1989.
29. Street, Anne Penfold, and Wallis, W. D. *Combinatorial Theory: An Introduction.* Winnipeg, Canada: The Charles Babbage Research Center, 1977.
30. Taubes, G. "Small Army of Code-breakers Conquers a 129-digit Giant." *Science* 264, 1994, pp. 776–777.
31. Trappe, Wade, and Washington, Lawrence C. *Introduction to Cryptography with Coding Theory*. Upper Saddle River, N. J.: Prentice-Hall, 2002.
32. Tucker, Alan. "Polya's Enumeration Formula by Example." *Mathematics Magazine* 47, 1974, pp. 248–256.

補充習題

1. 令 $f: G \to H$ 是一個群同態函數且 e_H 是 H 上的單位函數。證明
   a) $K = \{x \in G | f(x) = e_H\}$ 是 G 的子群。(K 被稱是同態函數的核集)
   b) 若 $g \in G$ 且 $x \in K$，則 $gxg^{-1} \in K$。
2. 若 G，H，和 K 是群且 $G = H \times K$，證明 G 有子群同構於 H 和 K。
3. 令 G 是一個群，其中 $a^2 = e$ 對所有 $a \in G$。證明 G 是可交換的。
4. 若 G 是一個偶階數的群，證明存在一個元素 $a \in G$ 滿足 $a \neq e$ 且 $a = a^{-1}$。
5. 令 $f: G \to H$ 是一個群同態映成 H。若 G 是一個循環群，證明 H 亦是循環的。
6. a) 考慮群 $(\mathbf{Z}_2 \times \mathbf{Z}_2, \oplus)$，其中對 a，b，c，$d \in \mathbf{Z}_2$，$(a, b) \oplus (c, d) = (a + c, b + d)$，和 $a + c$ 及 $b + d$ 以加法模 2 來計算，則 $(1, 0) \oplus (0, 1) \oplus (1, 1)$ 在此群中的值為何？
   b) 現考慮群 $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2, \oplus)$ 其中 $(a, b, c) \oplus (d, e, f) = (a + d, b + e, c + f)$。(此處和 $a + d$，$b + e$，$c + f$ 以加法模 2 來計算。) 當我們加此群中七個非零 (或非單位) 元素時，我們得到什麼？
   c) 敘述並證明一個含 (a) 和 (b) 之結果的一般化結果。
7. 令 $(G, \emptyset)$ 是一個群，其中
   $$x \circ a \circ y = b \circ a \circ c \Rightarrow x \circ y = b \circ c,$$
   對所有 a，b，c，x，$y \in G$。證明 $(G, \emptyset)$ 是一個交換群。
8. 對 k，$n \in \mathbf{Z}^+$，滿足 $n \geq k \geq 1$，令 $Q(n, k)$ 計數排列 $\pi \in S_n$ 的個數，其中 π 的任一表示式，一個互斥循環的乘積，不包含長度大於 k 的循環。證明
   $$Q(n+1, k) = \sum_{i=0}^{k-1} \binom{n}{i} (i!) Q(n-i, k).$$
9. 對 k，$n \in \mathbf{Z}^+$，其中 $n \geq 2$ 且 $1 \leq k \leq n$，令 $P(n, k)$ 表具有 k 循環的排列 $\pi \in S_n$ 的個數。[例如， (1)(23) 被計數於

$P(3, 2)$，(12)(34) 被計數於 $P(4, 2)$，且 (1)(23)(4) 被計數於 $P(4, 3)$。]

a) 證明 $P(n+1, k) = P(n, k-1) + nP(n, k)$。

b) 求 $\sum_{k=1}^{n} P(n, k)$。

10. 對 $n \geq 1$，若 $\sigma, \tau \in S_n$，定義 σ 和 τ 之間的距離 $d(\sigma, \tau)$ 為

$$d(\sigma, \tau) = \max\{|\sigma(i) - \tau(i)| | 1 \leq i \leq n\}.$$

a) 證明下面性質對 d 成立。

i) $d(\sigma, \tau) \geq 0$ 對所有 $\sigma, \tau \in S_n$。

ii) $d(\sigma, \tau) = 0$ 若且唯若 $\sigma = \tau$。

iii) $d(\sigma, \tau) = d(\tau, \sigma)$ 對所有 $\sigma, \tau \in S_n$。

iv) $d(\rho, \tau) \leq d(\rho, \sigma) + (\sigma, \tau)$ 對所有 $\rho, \sigma, \tau \in S_n$。

b) 令 ϵ 表 S_n 的單位元素 (亦即，$\epsilon(i) = i$ 對所有 $1 \leq i \leq n$)。若 $\pi \in S_n$ 且 $d(\pi, \epsilon) \leq 1$，那 $\pi(n)$ 值為何？

c) 對 $n \geq 1$，令 a_n 計數排列 π 在 S_n 的個數，其中 $d(\pi, \epsilon) \leq 1$，求並解一個遞迴關係給 a_n。

11. Wilson 定理 [16.1 節習題 19(d)] 告訴我們 $(p-1)! \equiv -1 \pmod{p}$，$p$ 為一質數。

a) 此定理的逆定理成立或不成立？亦即，若 $n \in \mathbf{Z}^+$ 且 $n \geq 2$，則 $(n-1)! \equiv -1 \pmod{n}$ 可得 n 是質數嗎？

b) p 是一個奇質數，證明

$$2(p-3)! \equiv -1 \pmod{p}.$$

12. 有多少個方法 Nicole 可塗圖 16.17 所示的正方形的八個區域，若

a) 有五種顏色可用？

b) 她確實恰使用五種可使用顏色中的四種？

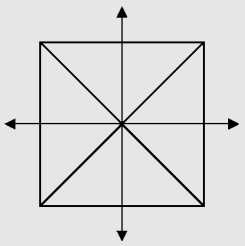


圖 16.17