平面近環、平衡不完全區組設計及密碼學

柯文峰

一. 引言

平面近環 (planar nearring) 是由 J. R. Clay 在 1968 年所提出。同一年, 另一位數學家 G. Ferrero 也正在研究有限整近環 (integral nearring) 的特性。而實際上, 一個有限整近環也就是一個有限的平面近環; 因此 Ferrero 的研究可以順利推展到平面近環上面。除此之外, Ferrero 也指出了有限整近環與平衡不完全區組設計 (balanced incomplete block design) 之間的關聯。自此之後的二十年間, 有好幾位數學家對平面近環及其在區組設計上做了研究, 但主要仍是由 Clay 來領導這一方面的研究工作。

Clay 和他的學生 M. Modisett 在 1988 年發現了一類能夠應用在密碼學 (Cryptography) 上的特殊平面近環與其所產生的區組設計。這一類區組設計有著類似於圓的特性; 也就是三個不同的點最多決定一個區組 (block)。

本文的目的在於介紹平面近環及其結構, 並說明如何將其應用在密碼學上。

二. 密碼學

簡單的說, 密碼學的目的在於研究如何保護資料的秘密性及完整性。當一份資料落入他人手中, 它的內容不爲其所了解, 這就是我們所謂的保護資料的秘密性。如何讓他人無法更改一份資料的內容 (資料經過非法更改之後會失去意義或是可以爲我們所測知) 則是所謂的保護資料的完整性。

一般的密碼系統有兩種: 傳統的及非傳統的密碼系統。傳統的密碼系統又稱爲對稱系統(Symmetric system), 也就是加密及解密 (enciphering and deciphering) 的鎖匙是相同的。而非傳統系的密碼則是在加密時所用的鎖匙與解密時所用的鎖匙並不相同, 因此加密的鎖匙可以公開。所以我們也稱此類系統爲公開鎖匙系統(public-key system)。圖一表示了一個對稱系統。

圖一. 對稱密碼系統

公開鎖匙系統最著名的例子是由 R. L. Rivest, A. Shamir 及 L. Adleman 三人所提出來的 RSA 密碼系統。此處我們並不準備多提。

底下我們以例子來說明對稱系統。

假設$\alpha = \{A, B, C, \cdots, X, Y, Z\}$而甲乙兩人準備用$\alpha$中的字母來溝通消息。甲、乙可以約定將各字母以順位移動 k 位的方式來編寫密文 $(1 \leq k \leq 25)$, 而 Z 順位移動一位得到的是 A。因此, 甲如何將"THECATISBLACK"送給乙呢? 假設他們約定 $k = 1$, 則甲將"UIFDBUJTCMBDL"送出, 因爲

$$\begin{array}{ccccccc} A & B & C & & X & Y & Z \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow \text{。} \\ B & C & D & & Y & Z & A \end{array}$$

當乙收到"UIFDBUJTCMBDL"時, 他則將每一字母逆向移一位而得知消息的內容。也就是說, 乙用以下的對應來得到原始資料:

$$\begin{array}{ccccccc} A & B & C & & X & Y & Z \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow \text{。} \\ Z & A & B & & W & X & Y \end{array}$$

這一個例子所用的加密方式並不能產生眞正保密的密碼。一個有經驗的密碼分析員人可以在研究幾十個字母之後就知道 k 的數值了。

我們再以一個例子來說明設計密碼時可能考慮的方向。

大家都知道在平面上任意不共線的三點可以決定唯一的一個圓, 而一個圓又可以用它的圓心和半徑來表示。因此我們可以設計如下的系統:

假設 $\mathcal{P}$ 爲一含有所有可能的明文 (plaintext) 的集合, 並且令 $f : \mathcal{P} \to \mathbf{C} \times \mathbf{R}^+$ 爲一個一對一的函數。對一個 $m \in \mathcal{P}$, 設 $f(m) = (m_c, m_r)$; 則我們可以從圓心爲 m_c 而半徑爲 m_r 的圓上取三個不同的點 x_m, y_m, z_m; 並將 (x_m, y_m, z_m) 定爲 m 之密文。當對方收到 (x_m, y_m, z_m) 時, 他只需找出包含有 (x_m, y_m, z_m) 的圓 (存在而且唯一), 取得其圓心和半徑, 再用 f^{-1} 來找回原來的明文。

這個系統並不實際, 因爲 (1) x_m, y_m 及 z_m 都可能不爲有理數, 因此在表達上出現困難。(2) 如果一個窺視者知道了編碼法 (也就是由圓上取三個點), 則他也很容易可以得到圓心及半徑, 進而導出明文。

第一個問題說明了實用性的考慮是必要的, 而第二個問題則導致是否應該將一個編碼法加以保密的問題。一般來說, 研究密碼學的人都會有個相同的信念, 也就是說: 一個

密碼系統的安全性不應該是只建立在編碼方法的保密上。所以在討論一個密碼系統的安全性時我們都是假設要破解此一系統的人只是不知道正確的鎖匙而已。因此一個具有衆多不同鎖匙的密碼系統是比較安全的。

雖然上面的例子並不實際, 但仍有其優點。我們用此法來編密碼時, 可以任意選取圓上的三個點, 而這種組合在平面上可以有無窮多種。如此一來, 明文與密文之間就比較沒有關係。可是不論密文是什麼, 明文一樣可以被正確的導出來。

現在的問題是, 是否可以找到又實用, 又具有像圓的特性的結構來供我們使用呢? 我們的答案是肯定的, 而且這種代數結構很容易可以得到。

三. 平面近環

我們以爲數學不止是解決實際問題之鑰, 它本身也是美的一種表徵。雖然我們可以忽略底下的討論而直接去製造我們所需要的區組設計以供密碼系統的使用, 但如此一來, 人們將不會完全了解如此設計的原因, 並且錯失了一個非常漂亮的代數結構。因爲平面近環所表達的正是一種在不對稱的世界中的對稱現象。

首先我們定義所謂的近環(nearring)。一個近環是一個具有兩種二元運算的集合 N。這兩種二元運算通常記成 $+$ 及 $\cdot$, 並且它們會滿足底下的性質:

(1) $+$ 及 $\cdot$ 皆滿足結合律;

(2) 對 $+$ 存在有一單位元 0 使得對所有 N 中的元素 x, $0+x=x+0=x$ 永遠滿足;

(3) 對任意的 x, 可以找到另一個元素 x' 使得 $x+x'=x+x'=0$, 通常 x' 被稱爲 x 的反元素並記成 $-x$;

(4) $\cdot$ 對 $+$ 有右邊分配律: 對任意之 x, y, z, 有 $(x+y)\cdot z = x\cdot z + y\cdot z$。

以上的 (1), (2) 及 (3) 說明了 $(N,+)$ 是一個群 (group), 而 $(N,\cdot)$ 是一個半群 (semigroup)。由於是滿足了右手分配律, 我們稱這種近環爲右手近環。如果將右手分配律以左手分配律來取代, 則我們得到的是左手近環。左、右手近環的理論裡是平行的。

近環的例子隨處都是。比如說大家所熟知的有理數、實數及複數都是近環。但是這些例子都有太強的條件, 並不適合用來做爲近環的例子。要得到沒有另一邊分配律的"眞正近環"的例子, 可以將所有整係數的多項式收集起來, 記爲$\mathbf{Z}[\mathbf{x}]$; 取一般之加法爲 $+$, 而用函數合成 $\circ$ 爲其乘法 (也就是將多項式看爲函數), 如此則得到一個沒有左邊分配律的近環 $(\mathbf{Z}[\mathbf{x}],+,\circ)$。

在任意的 (右手) 近環 $(N,+,\cdot)$ 上, 我們可以定義一個對等關係 $=_m$:

$a=_m b$ 若且唯若對任意之 x, $xa=xb$ 恆成立。現在, 我們可以將平面近環的定義寫下來: 我們稱一個近環 $(N,+,\cdot)$ 爲平面近環如果 (1) $N/=_m$ 最少有三個對等類 (2) 如果 $a,b,c\in N$ 且 $a\neq_m b$, 則方程式 $xa=xb+c$ 有唯一解。

底下的三個平面近環的例子是由 G. Anshel 在 1968 年提出來的。

1. 在$\mathbf{C}$ 上定義一個新的乘法 $*_1$:

$$b *_1 a = \begin{cases} a_1 b, & \text{若 } a = a_1 + a_2 i \\ & \text{且 } a_1 \neq 0; \\ a_2 b, & \text{若 } a = a_2 i。 \end{cases}$$

此處 a_1 及 a_2 皆爲實數。如此則 $(\mathbf{C},+,*_1)$ 爲一平面近環。

2. 在$\mathbf{C}$上定義另一個乘法 $*_2$:

$$b *_2 a = |a|\, b。$$

則 $(\mathbf{C},+,*_2)$ 爲一個 $*$ 平面近環。

3. 在$\mathbf{C}$上定義乘法 $*_3$ 爲

$$b *_3 a = \begin{cases} 0, & \text{若 } a = 0; \\ \frac{a}{|a|} b, & \text{若 } a \neq 0。 \end{cases}$$

則 $(\mathbf{C},+,*_3)$ 也是一個平面近環。

在下一節結束後我們會有更多平面近環的例子。

四. 平面近環的特徵刻劃

這一節裡的結果是由 Ferrero 在 1968 年所作的。

令 $(N,+,\cdot)$ 爲一平面近環。取 N 中任一元素 x。如果 $x \neq_m 0$, 則定義一個函數 $\phi_x : N \to N$; $\phi_x(y) = yx$。則 ϕ_x 有以下之性質:

(1) ϕ_x 爲群 $(N,+)$ 的一個自同構 (automorphism); 也就是說, ϕ_x 爲一個一對一的映成函數, 並且 $\phi_x(y+z) = \phi_x(y) + \phi_x(z)$。

(2) 如果 ϕ_x 不是 N 之恆等函數 id_N 則 $\phi_x(y) = y$ 只在 $y = 0$ 時成立。

(3) 如果 $\phi_x \neq id_N$, 則 $-\phi_x + id_N$ 爲一個映成函數。

此時, 若將 Φ 定爲 $\Phi = \{\phi_b | b \in N,\ b \neq_m 0\}$, 則 Φ 是 $(N,+)$ 的一個自同構群 (group of automorphisms)。

反之, 如果我們有一個群 $(G,+)$ 以及一個 G 之自同構群 Φ, 而且 Φ 的元素滿足了以上之 (2) 與 (3) 的條件, 則由以下的步驟可以在 G 上定出一個二元運算 $\cdot$ 使得 $(G,+,\cdot)$ 成爲一個平面近環。

步驟一: 計算所有 Φ 在 G 上的軌跡 (orbit)。對任一 G 之元素 x, $\Phi(x) = \{\varphi(x) | \varphi \in \Phi\}$ 即是 Φ 之一個軌跡。令 $\mathcal{B} = \{\Phi(a) | a \in G,\ a \neq 0\}$。

步驟二: 取 $\mathcal{B}$ 之任一個非空子集合 $\mathcal{C}$, 並令 $A = G \backslash (U\mathcal{C})$。

步驟三: 將 $\mathcal{C}$ 中的所有軌跡的代表元固定。如果 $c \in \mathcal{C}$, 將這個代表元記爲 e_c。

步驟四: 定義 G 上之二元運算 $\cdot$ 如下:

$$b \cdot a = \begin{cases} 0, & \text{若 } a \in A; \\ \phi(b), & \text{若 } a \in c,\ c \in \mathcal{C} \\ & \text{且 } \phi(e_\circ) = a。 \end{cases}$$

如此一來, $(G,+,\cdot)$ 成爲一個平面近環。

由 Ferrero 的結果, 我們很容易找到平面近環。在這一個平面近環的刻劃裡, 一個平面近環 $(N,+,\cdot)$ 可以對應到兩個群 $(N,+)$

及 $(\Phi, 0)$, 因些我們將 (N, Φ) 稱爲一個 Ferrero 序對 (Ferrero pair)。但是我們必須注意到的是, 由一個 Ferrero 序對所能產生的平面近環並不是唯一的, 它和步驟二中 $\mathcal{C}$ 的選取, 以及步驟三中代素元的選取都有關係。

接下來, 我們可以製造出許多平面近環。我們需要的材料是體 (field)。

取一個體 $(F, +, \cdot)$。令 $F^* = F\backslash\{0\}$, 則 $(F^*, \cdot)$ 是一個群。假計 Φ' 是 F^* 的一個子群且 $|\Phi'| \geq 2$。如果 $a \in \Phi'$, 定義一個函數 $f_a : F \to F$; $f_a(b) = b \cdot a$。則 f_a 滿足了 (1) 和 (2), 而且 $\Phi = \{f_a | a \in \Phi'\}$ 是和 Φ' 同構 (isomorphic) 的一個 $(F, +)$ 的自同構群, 也就是說 (F, Φ) 是一個 Ferrero 序對。因此在 $(F, +)$ 上可以重新定義許多二元運算使得 F 成爲平面近環。

事實上, Anshel 所提供的三個例子 $(\mathbf{C}, +, *_1)$, $(\mathbf{C}, +, *_2)$ 和 $(\mathbf{C}, +, *_3)$ 都是如此定義出來的。在 $(\mathbf{C}, +, *_1)$ 的情形裡, Φ' 取的是 $\mathbf{R}\backslash\{0\}$; 在 $(\mathbf{C}, +, *_2)$ 的情況中, Φ' 取的是 $\mathbf{R}^+ = \{r \in \mathbf{R} | r > 0\}$; 而在最後一個 $(\mathbf{C}, +, *_3)$ 中, Φ' 則是取爲平面上的單位圓。

再舉一個簡單的例子。取 t 個元素的體 $\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, 令 $\Phi' = \{1, 2, 4\}$。所以 $\Phi = \{f_1, f_2, f_4\}$。Φ 有三個軌跡, 分別是

$$\Phi(0) = \{0\},\ \Phi(1) = \{1, 2, 4\}$$
$$\text{和 } \Phi(3) = \{3, 6, 5\}。$$

取 $\mathcal{C} = \{\Phi(1)\}$ 並定 2 爲 $\Phi(1)$ 的代表元, 因此

$$1 = f_4(2),\ 2 = f_1(2),\ 4 = f_2(2),$$

而 $\mathbf{Z}_7$ 上的二元運算則是定爲

$*$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	4	1	0	2	0	0
2	0	1	2	0	4	0	0
3	0	5	3	0	6	0	0
4	0	2	4	0	1	0	0
5	0	6	5	0	3	0	0
6	0	3	6	0	5	0	0

如此, 則 $(\mathbf{Z}_7, +, *)$ 即爲一個平面近環。

五. 平衡的不完全區組設計

平衡的不完全區組設計起源於農業實驗設計, 今日則自成組合學中熱門研究題材之一, 並且在許多方面有所應用。

什麼是平衡的不完全區組設計呢? 它是一個有限集合 X 以及 X 的一個子集合的集合 $\mathcal{B}$ 所形成。$\mathcal{B}$ 必須滿足以下的條件:

(1) 每一個區組 $B \in \mathcal{B}$ 有固定數目的元素,

(2) 每一個 X 的元素必定包含有一個固定數目的區組之中

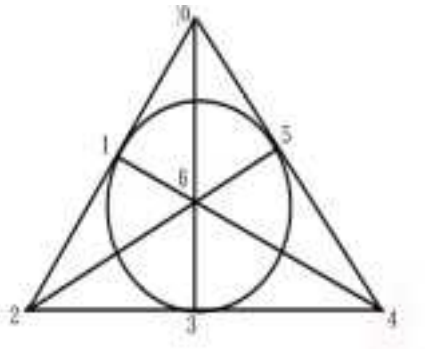
(3) 每一對 X 的元素必須包含在一個固定數目的區組中。

最著名的例子當屬於底下的這一個。

$$X = \{0, 1, 2, 3, 4, 5, 6\},$$

$$\mathcal{B} = \{\{0,1,2\},\{0,3,6\},\{0,4,5\},\{1,3,5\},\{1,4,6\},\{2,3,4\},\{2,5,6\}\}。$$

通常以圖形表示:



平面近環和平衡的不完全區組設計又有什麼關係呢? Clay 在他 1988 年的一篇論文中證明了下面的定理。

令$(N,+,\cdot)$爲一個有限的平面近環。如果 $a,b \in N$,$a \neq 0$, 則定義 $N^*a+b = \{na+b | n \neq_m 0\}$。取 $\mathcal{B} = \{N^*a+b | a \in N,\ a \neq 0\}$, 則 $(N,\mathcal{B})$ 是一個平衡的不完全區組設計。

事實上, 如果 (N,Φ) 是 N 的相關 Ferrero 序對, 則每一個 N^*a+b 就是 $\Phi(a)+b = \{\varphi(a)+b | \varphi \in \Phi\}$。因此 $|N^*a+b| = |\Phi|$。而且, 每一個 N 的元素都屬於 $|N|-1$ 個區組, 而每兩個不同的元素則屬於 $|\Phi|-1$ 個區組。

Clay 的定理說明了平面近環是平衡的不完全區組設計的一個很好的來源。

現在我們回顧一下 Anshel 的第三個例子 $(\mathbf{C}, +, *_3)$。在這個平面近環裡, 每一個 $\mathbf{C}^* *_3 a+b$, $a \neq 0$, 都是一個圓, 而其圓心及半徑則分別是 b 及 $|a|$。由於一個圓可以爲其上的任意三個點所唯一決定, Clay 因此考慮是否在一般的平面近環上這種情況仍然成立。很快的他就發現了事情並非如此。但是事情也不是全然無望, 因爲某些平面近環具備了三點最多決定一個區組的特性, 而這也是有限平面近環所能擁有的最接近於圓的性質了。所以這種平面近環就被稱爲具有圓性的 (circular) 平面近環 (也就是圓性平面近環)。反之, 如果一個平衡不完全區組設計有 (1) 兩點最少屬於兩個以上之區組, 及 (2) 三點最多決一個區組, 則我們稱之爲具有圓性的。現在, 如果一個 Ferrero 序對 (N,Φ) 所決定的平衡的不完全區組設計是具有圓性的, 則我們也將之稱爲具有圓性的, 也就是說 (N,Φ) 爲具圓性的 Ferrero 序對。

爲了深入探究這種特殊的代數結構, Clay 寫了一個電腦程式來決定了所有可能的圓性 Ferrero 序對 $(\mathbf{Z}_p,\Phi_k)$, p 則是小於 1000 的所有質數, 而 k 整除 $p-1$。但是若要有實用性, 則下面的定理更爲適當。

定理(Modisett; 1988): 對任意的正整數 k, $k \geq 3$, 存在有一個質數的有限集合 $\mathcal{P}_k$ 滿足了下面的性質: 假如 F 是一個有限體且 $k|(|F|-1)$, 令 Φ_k 爲 F^* 的子群, $|\Phi_k| = k$。則 Ferrero 序對 (F,Φ_k) 是具有圓性的充分必要條件是 F 的特徵值不在 $\mathcal{P}_k$ 中。

除了定理本身的漂亮之外, 更重要的是 $\mathcal{P}_k$ 也有方法可以決定。底下所列的是前八個

$\mathcal{P}_k$, $k = 3, 4, \cdots, 10$。

$$\begin{aligned}
\mathcal{P}_3 &= \{3\} \\
\mathcal{P}_4 &= \{2, 5\} \\
\mathcal{P}_5 &= \{5, 11\} \\
\mathcal{P}_6 &= \{2, 3, 7, 13, 19\} \\
\mathcal{P}_7 &= \{2, 7, 29, 43\} \\
\mathcal{P}_8 &= \{2, 3, 5, 17, 41\} \\
\mathcal{P}_9 &= \{3, 19, 37, 73, 109, 127, 271\} \\
\mathcal{P}_{10} &= \{2, 5, 11, 31, 41, 61, 71, 101\}。
\end{aligned}$$

六. 密碼系統之建構

在第一節中, 我們舉了一個利用圓的特性來"保密"的例子。我們也說明了那是一個不切實際的例子而已。其中一個原因是大家都知道如何在複數平面上以三點來決定出唯一的圓。如果我們用的是一個特殊的圓性平面近環來作相同的事, 則會如何? 結果是除非一個人知道密碼是使用那一個平面, 否則他必須花更大的功夫來解讀, 甚至根本無法解讀也是可能的。

另一個原因是複數的表達方式並不適合用在現實世界之中。要是我們使用有限體, 甚至是 $\mathbf{Z}_p$ (p 爲質數), 來做爲密碼系統之根本, 則一切資訊將是以整數的方式來表達, 因此沒有複數的困擾。

最後要考慮的是這類特殊平面近環的來源是否充裕, 換句話說, 是否能夠很容易就建立起來? 這點可以用 Modisett 的定理來回答。由於對一個 k, $\mathcal{P}_k$ 都是有限的, 所以只要找到夠大的質數 p 使得 $p \in \mathcal{P}_k$ 且 $k|(p-1)$, 則 $(\mathbf{Z}p, \Phi_k)$ 就會具有圓性。因此, 圓性平面近環在密碼系統的應用上, 應該是有所爲的。

底下我們就來描述如何去建構一個利用平面近環的密碼系統。

假設甲和乙兩人要建立一個安全的消息傳送管道。首先他們決定了要使用那一個圓性平面近環, 也就是說他們必須同意一組 (p, k), p 是一個質數而 $k|(p-1)$, 並且 $(\mathbf{Z}_p, \Phi_k)$ 是一個圓性 Ferrero 序對。

接下來, 甲和乙同意如何將消息 (譬如說是由 26 個英文字母加上空格及標點符號) 轉成小於 p 的數字。一般來說, 這轉換方法都是直接的。

最後, 甲和乙同意只使用含有一個固定元數 $x_0 (0 \le x_0 \le p-1)$ 的所有區組, (共有 $p-1$ 個), 它們是 $\Phi_k(n) + (x_0 - n)$, $n = 1, 2, \cdots, p-1$。

如果甲要將一訊息, 例如 m, 通知乙, 甲就將 m 轉換成數字, 比如說是 a_m; 再從區組 $\Phi_k(a_m)+(x_0-a_m)$ 中任意挑出兩個異於 x_0 的數, 比方說是 b_m 和 c_m; 然後將 (b_m, c_m) 發送出去給乙。

當乙接收到 (b_m, c_m) 後, 他就在所有的 $\Phi_k(n)+(x_0-n)$ 中去尋找包含有 b_m 及 c_m 的區組。當然這一個區組是唯一存在, 而且剛好就是 $\Phi_k(a_m) + (x_0 - a_m)$。由此, 乙可以由 a_m 推知 m 而知道甲要他知道的消息了。

我們舉一個簡單的例子來說明上面的步驟。

假設甲、乙二人決定了要用 $p = 31$, $k = 5$ (由 Modisett 的 $p_5 = \{5, 11\}$ 我們知道 $(\mathbf{Z}_{31}, \Phi_5)$ 是具有圓性的)。並且他也

同意使用含有數字 10 的 30 個區組 $\Phi_5(n)+(10-n)$, $1 \le n \le 30$, 來傳送 26 個字母, 空格以及四個標點符號 ，, ．, ； 和“。這些符號則是用下面的對應轉成小於 31 的整數:

$A \leftrightarrow 1, B \leftrightarrow 2, \cdots, X \leftrightarrow 24, Y \leftrightarrow 25, Z \leftrightarrow 26$, 空格$\leftrightarrow 27$, ，$\leftrightarrow 28$, ．$\leftrightarrow 29$, ；$\leftrightarrow 30$, “ $\leftrightarrow 0$。

下面是計算後的 30 個區組 $\Phi_k(n)+(10-n)$, $1 \le n \le 30$:

$\Phi_5 = \{1,2,4,8,16\}$
$\Phi_5(1) + (10-1) = \{10,11,13,17,25\}$
$\Phi_5(2) + (10-2) = \{9,10,12,16,24\}$
$\Phi_5(3) + (10-3) = \{0,10,13,19,24\}$
$\Phi_5(4) + (10-4) = \{7,8,10,14,22\}$
$\Phi_5(5) + (10-5) = \{10,14,15,23,25\}$
$\Phi_5(6) + (10-6) = \{7,10,16,21,28\}$
$\Phi_5(7) + (10-7) = \{0,10,17,22,28\}$
$\Phi_5(8) + (10-8) = \{3,4,6,10,18\}$
$\Phi_5(9) + (10-9) = \{6,10,11,19,21\}$
$\Phi_5(10) + (10-10) = \{5,9,10,18,20\}$
$\Phi_5(11) + (10-11) = \{10,12,20,21,25\}$
$\Phi_5(12) + (10-12) = \{1,4,10,15,22\}$
$\Phi_5(13) + (10-13) = \{8,10,18,19,23\}$
$\Phi_5(14) + (10-14) = \{3,10,15,21,24\}$
$\Phi_5(15) + (10-15) = \{10,18,22,24,25\}$
$\Phi_5(16) + (10-16) = \{2,10,26,27,29\}$
$\Phi_5(17) + (10-17) = \{5,10,17,27,30\}$
$\Phi_5(18) + (10-18) = \{1,2,10,12,28\}$
$\Phi_5(19) + (10-19) = \{5,10,16,19,29\}$
$\Phi_5(20) + (10-20) = \{0,8,10,26,30\}$
$\Phi_5(21) + (10-21) = \{0,2,10,11,15\}$
$\Phi_5(22) + (10-22) = \{1,9,10,14,30\}$
$\Phi_5(23) + (10-23) = \{2,10,14,16,17\}$
$\Phi_5(24) + (10-24) = \{3,10,20,23,29\}$
$\Phi_5(25) + (10-25) = \{4,10,13,23,30\}$
$\Phi_5(26) + (10-26) = \{5,6,10,26,28\}$
$\Phi_5(27) + (10-27) = \{6,10,12,13,29\}$
$\Phi_5(28) + (10-28) = \{1,7,10,20,27\}$
$\Phi_5(29) + (10-29) = \{4,8,10,11,27\}$
$\Phi_5(30) + (10-30) = \{3,7,9,10,26\}$

現在, 如果甲要把句子

THE CAT IS BLACK

通知乙, 甲就將它轉成

19,8,5,27,3,1,19,27,9,18,27,2,12,1,3,11,

29

然後從相關的區組 $\Phi_5(19) + (10-19)$, $\Phi_5(8)+(10-8), \cdots, \Phi_5(29)+(10-29)$。中分別選出兩個適當的數字而將下面的數列傳送給乙。

5,16,6,18,14,15,13,29,24,0,25,17,19,29,

13,10,11,19,1,2,6,12,12,9,1,4,11,17,0,

24,12,21,4,27。

當乙收到以上的數列時, 他就到 $\Phi_5(n) + (10-n)$ 的表中找出相對的 a_m 值, 反推而得到甲所要傳送的消息了。

當然這個簡單的例子不是十分保密, 但是它說明了如何以使用平面近環來建立保密的通訊管道。爲了要使系統安全, 我們必須使用較大的 p 及 k。可是當 p 和 k 增大時, 解

碼法就必須加以適當設計而不能再以查表的方式來做了。要設計出好的解碼方法, 則必須對平面近環與區組設計之間的關聯有更爲深入的瞭解才行。

七. 結論

在以上的密碼系統討論裡, 我們沒有對我們的系統做深入的分析或是討論其它可能的建構方式, 因爲這不是本文的眞正目的。我們所要表達的觀念是: 純數的研究不一定會和應用脫節。平面近環在它的二十多年發展歷史中已經表達了它在純數與應用方面的卓越貢獻。它的起源則完全是由於 Clay 對新的代數結構的好奇而引起。另一方面, 平衡的不完全區組設計則是因爲農業實驗設計所需而發展出來。今日, 它不僅是在實驗設計及統計上有用, 也在編碼學上有重大貢獻, 而且它本身也是組合學裡的一個熱門研究方向。由於平面近環理論的研究, 這個奇特的區組設計也多了一個應用、研究的方向。

參考文獻

[1] G. Betsch and J. R. Clay, Block designs from Frobenius groups and planar near-rings, Proc. Conf. Finite Groups (Park City, Utah), 1976, Academic Press, 473 -502.

[2] J. R. Clay, Generating balanced incomplete block designs from Frobenius groups, Discrete Math. 59 (1972), 229-234.

[3] J. R. Clay, Circular block designs from planar nearrings, Annals of Discrete Math., 37 (1988), 95-106.

[4] J. R. Clay, Geometric and combinatorial ideas related to circular planar nearrings, Bulletin of the Institute of Mathematics Academia Sinica, 16 (1988), 275-283.

[5] J. R. Clay, Compound closed chains in circular planar nearrings, Annals of Discrete Mathematics, 1992.

[6] J. R. Clay, Nearrings: Geneses and Applications, Oxford Univrsity Press, Oxford, 1992.

[7] J. R. Clay and Y. N. Yeh, On some geometry of Mersenne primes, to appear in Studia Scientiarun Mathematicarum Hugarica.

[8] P. Fuchs, G. Hofer and G. Pilz, Codes from planar near-rings, IEEE Trans. on Information Theory, 36 (1990).

[9] W. F. Ke, Structures of Circular Planar Nearrigs, Ph. D. dissertation, University of Arizona, Tucsan, 1992.

[10] M. C. Modisett, A characterization of the circularity of certain balanced incomplete block designs, Ph. D. dissertation, University of Arizona, Tucsan, 1988.

—本文作者任教於成功大學應用數學研究所—