希爾伯特第十問題

游 淑 敏
板橋高中數學教師

December 26, 2004

目 錄

前言

1900 年德國大數學希爾伯特 (Hilbert) 在巴黎的國際數學大會上提出了有名的 23 個數學問題集，而第十問題就是其中精彩的一個，其內容為：“判定任意整係數刁藩圖方程式是否有整數解”。即要求給出一個演算法，使得透過此演算法的運算後，可判定任意刁藩圖方程式是否有整數解。

這個問題已在 1970 年得到否定的答案。希爾伯特第十問題的解決 是集體的智慧，令人驚奇的是僅用了一些數理邏輯和初等數論就解決了這一大難題。本論文將深入淺出的介紹這七十年間 $(1900-1970)$，有關第十問題的進展、演變及研究情況。

關於解一個特定的刁藩圖方程式，是一個既古老且重要的數學問題，例如判定二元一次刁藩圖方程式 $ax+by=c$ 是否有整數解與判定 a,b 的最大公因數是否能整除 c 是等價的，這可透過大家所熟悉的歐基里得輾轉相除法來完成。某些特殊的二元二次刁藩圖方程式，例如：貝爾 (Pell) 方程式 $x^2-dy^2=1, x^2-mxy+y^2=1$，人們甚至可以寫下它們的公式解，但對於多元或者是高次的刁藩圖方程式，證明它們是否有整數解，或是求出它們的整數解，並不是一件容易的事。

美國數學家戴維斯 (Davis)、魯賓遜 (Robinson)和 普特南 (Putnam)在第十問題的征途上，作了許多偉大的貢獻，而臨門的一腳是在 1970 年時，由俄國年輕數學家馬吉雅塞維奇 (Matiyasevich)在蘇聯科學院院報上，發表的著名論文 [10]：《遞歸可枚舉集是刁藩圖的》，進而得到了第十問題的不可解答案。

在1930年間提出了第十問題是不可解的預測，並造成遞歸理論與可計算理論的蓬勃發展。由此兩理論所產生的可計算函數及遞歸函數與第十問題的刁藩圖函數有很密切的關係。事實上，我們將證明這三大類函數是等價的。

由於目前所知的演算法模型都等價於圖靈機演算法，所以第一章中，由圖靈機所定義的可計算函數可視為演算法所產生的函數。在圖靈機的相關理論中，我們得到兩個重要運算：複合運算與最小化運算。這兩個運算對可計算函數都是滿足封閉性的，這樣的性質使可計算函數變得更豐富、多樣。而遞歸函數在解決第十問題的過程中亦扮演很重要的角色。所謂遞歸函數是由函數：

$$C(x)=1, S(x)=x+1, x+y, x\dot{-}y, xy, U_i^n(x_1,\cdots,x_n)=x_i, 1\le i\le n$$

透過複合運算及最小化運算所生成的函數。利用中國剩餘定理、整數的配對函數及序對函數，可得到遞歸函數的另一個等價定義：由下列函數

$$C(x)=1, N(x)=0, S(x)=x+1, U_i^n(x_1,\cdots,x_n)=x_i, i=1,\cdots,n$$

透過複合、最小化及原始遞歸運算所生成的函數。此等價定義讓我們獲得更多關於（原始）遞歸敘述的相關性質，進而得到：一個函數是可計算的充份必要條件是它是遞歸的。

解決希爾伯特第十問題的重要關鍵，就是證明冪函數 x^y 是刁藩圖的。1952年， 魯賓遜 [17]證明了函數

$$\binom{x}{y}, x!, \prod_{k=1}^{y}(a+bk)$$

及受囿量詞 $(\forall k)_{\le y}$ 都是指數刁藩圖的，也給出了質數所成集合的指數刁藩圖表現。又利用貝爾方程式

$$x^2-dy^2=1$$

的豐富性質，提出一個假設（魯賓遜假設）：設存在刁藩圖敘述 $u(x,y)$ 滿足

(1) 若整數 $x,y\geq 0$ 使得 $u(x,y)$ 成立，則 $y<x^x$,

(2) 對任意的整數 $k\geq 0$，存在整數 $x,y\geq 0$ 使得：敘述 $u(x,y)$ 成立且 $y\geq x^k$,

則冪函數 x^y 可表成若干個刁藩圖方程式的聯立方程組，也就是說，敘述 $z=x^y$ 是刁藩圖的，即指數刁藩圖集與一般的刁藩圖集是等價的。

馬吉雅塞維奇 [10]於 1970 年利用斐波那契數列

$$u_0=1,u_1=u_2=1,u_{n+2}=u_{n+1}+u_n$$

找到了滿足魯賓遜假設的敘述，並證明了冪函數 x^y 是刁藩圖的。此重要結果讓我們確定函數

$$\binom{x}{y},x!,\prod_{k=1}^{y}(a+bk)$$

及受囿量詞 $(\forall k)_{\leq y}$ 都是刁藩圖的，進而得到：指數刁藩圖集與刁藩圖集是等價的及一個全函數是刁藩圖的充份必要條件是它是遞歸函數等兩個重要結果。

1961年，戴維斯、普特南與魯賓遜 [4] 證明了通用刁藩圖方程式的存在。（1975年，馬吉雅塞維奇與魯賓遜[13] 確實構造了通用刁藩圖方程式）。利用通用刁藩圖方程式，我們可找到了一個 1 維的刁藩圖集 S，其餘集 $N-S$ 不是刁藩圖的。利用此集合的特徵函數不是遞歸函數（當然也不是可計算函數），最後終於證明了希爾伯特第十問題的否定性答案。

第 1 章

可計算函數 (Computable Functions)

本章的目的是透過圖靈機來定義及討論可計算函數的性質，我們可以證明可計算函數對複合運算及最小化運算是封閉的。

1.1 圖靈機

一個 四元數列(quadruple) 是指由下列符號

$$q_1, q_2, q_3, \cdots, S_0, S_1, S_2, \cdots, R, L$$

所構成且符合下列其中一種形式的有限數列：

(1) $q_i S_j S_k q_l$.

(2) $q_i S_j R q_l$.

(3) $q_i S_j L q_l$.

例如：$q_1 S_0 S_1 q_2, q_3 S_5 R q_2, q_4 S_5 L q_1$ 都是四元數列。

一個表示式 (expression) 是指由下列符號

$$q_1, q_2, q_3, \cdots, S_0, S_1, S_2, \cdots$$

所構成的一串有限數列，此數列只能包含唯一的一個 q_i，且此 q_i 不可位於數列的最右邊。例如：

$$q_1 S_2 S_3 S_0, S_1 S_0 q_3 S_0 S_8 S_1 S_2$$

都是表示式。

定義 **1.1** 設 Z 是一個由四元數列所構成的有限集合，如果 Z 中任意兩個四元數列的前兩個元素 $q_i S_j$ 皆不一樣，則稱 Z 是一個 圖靈機(Turing Machine)。

例如集合

$$Z = \{q_1 S_1 S_0 q_1\ ,\ q_1 S_0 R q_2\ ,\ q_2 S_1 R q_2\ ,\ q_2 S_0 L q_3\ ,\ q_3 S_1 S_0 q_3\},$$

就是一個圖靈機。

為了方便起見，我們把元素 q_i 稱為 q-元素，元素 S_i 稱為 S-元素，一個由 S-元素所構成的有限數列（包括空數列）稱為 S-數列。

定義 **1.2** 設 Z 是一個圖靈機。若表示式 α, β 滿足下列其中的一種情況，我們就以符號

$$\alpha \to \beta\,(Z)$$

來表示。

(1) 存在 S-數列 P 及 Q 使得 α 為 Pq_iS_jQ，β 為 Pq_lS_kQ，且 $q_iS_jS_kq_l \in Z$。

(2) 存在 S-數列 P 及 Q 使得 α 為 $Pq_iS_jS_kQ$， β 為 $PS_jq_lS_kQ$，且 $q_iS_jRq_l \in Z$。

(3) 存在 S-數列 P 使得 α 為 Pq_iS_j， β 為 $PS_jq_lS_0$，且 $q_iS_jRq_l \in Z$。

(4) 存在 S-數列 P 及 Q 使得 α 為 $PS_kq_iS_jQ$， β 為 $Pq_lS_kS_jQ$，且 $q_iS_jLq_l \in Z$。

(5) 存在 S-數列 Q 使得 α 為 q_iS_jQ，β 為 $q_lS_0S_jQ$，且 $q_iS_jLq_l \in Z$。

對表示式 α 而言，若不存在表示式 β 使得 $\alpha \to \beta\,(Z)$ 成立，則稱表示式 α 是圖靈機 Z 的一個<u>終結式</u>。

由定義 1.2 可知，若表示式 α 不是 Z 的一個終結式，則僅存在唯一的表示式 β 使得 $\alpha \to \beta(Z)$ 成立。因為若存在相異的表示式 β_1, β_2 使得 $\alpha \to \beta_1\ (Z), \alpha \to \beta_2\ (Z)$ 皆成立，則圖零機 Z 存在了兩個相異且前兩個元素 q_iS_j 相同的四元數列，此與定義 1.1 矛盾。

元素 S_0, S_1 在本章的各節中，扮演著很重要的角色，為了方便起見，我們以符號 B 代表 S_0，以符號 1 代表 S_1。對任意非負整數 n， 我們以符號 $\overline{n}$ 代表 $n+1$ 個 1 所構成的 S-數列，以符號 $\overline{n_1, n_2, \cdots, n_k}$ 代表 S-數列 $\overline{n_1}B\overline{n_2}B\cdots B\overline{n_k}$。例如 $\overline{3} = 1111$， $\overline{2,3,0} = \overline{2}B\overline{3}B\overline{0} = 111B1111B1$。

定義 **1.3** 設 M 是一個表示式，符號 $\langle M\rangle$ 代表 1 在 M 中出現的次數。

例如：$\langle 11BS_4q_3B\rangle = 2, \langle q_3S_2S_5\rangle = 0, \langle q_2\overline{n-1}\rangle = n$。

設 Z 是一個圖靈機，α_1 是一個表示式。若存在有限個表示式 $\alpha_2, \cdots, \alpha_n$ $(n \geq 2)$ 使得

$$\alpha_i \to \alpha_{i+1}(Z),\ \ 1 \leq i < n,$$

且 α_n 是 Z 的一個終結式，則稱 α_1 對 Z 存在著<u>算式</u>，我們以 $\mathrm{Res}_Z(\alpha_1)$ 來代表此算式的終結式 α_n；反之，則 α_1 對 Z 不存在著算式， $\mathrm{Res}_Z(\alpha_1)$ 沒有定義。

在此後的各章節中，以符號 N 代表所有非負整數所構成的集合。

定義 **1.4** 設 Z 是一個圖靈機， n 維函數

$$\psi_Z^{(n)}(x_1, \cdots, x_n)$$

定義如下：設表示式 $\alpha_1 = q_1\overline{m_1, \cdots, m_n}$, $m_1, m_2, \cdots, m_n \in N$
(1) 若 α_1 對 Z 存在著算式，則函數值

$$\psi_Z^{(n)}(m_1, \cdots, m_n) = \langle \mathrm{Res}_Z(\alpha_1)\rangle;$$

(2) 若 α_1 對 Z 不存在著算式，則 $\psi_Z^{(n)}(m_1, \cdots, m_n)$ 沒有定義，也就是序對 $(m_1, \cdots, m_n)$ 不在函數 $\psi_Z^{(n)}(x_1, \cdots, x_n)$ 的定義域內。

我們常將函數 $\psi_Z^{(1)}(x)$ 簡寫為 $\psi_Z(x)$。

1.2 可計算函數及其例子

定義 **1.5** 若函數 $f(x_1,\cdots,x_n)$ 是一個 全函數（即定義域為 N^n 的函數），且存在一個圖靈機 Z 使得

$$f(x_1,\cdots,x_n)=\psi_Z^{(n)}(x_1,\cdots,x_n),$$

則稱函數 $f(x_1,\cdots,x_n)$ 是一個可計算函數 (computable function)，或稱函數 f 是 可計算的。

由定義 1.5 可知，可計算函數 $f(x_1,\cdots,x_n)$ 的定義域是 N^n，值域是 N 的一個子集合。以下是幾個可計算函數的例子：

例題 **1.1** 函數 $A(x,y)=x+y$ 是可計算的。設圖靈機

$$Z_A=\{q_11Bq_1,\ q_1BRq_2,\ q_21Rq_2,\ q_2BRq_3,\ q_31Bq_3\}.$$

表示式 $\alpha_1=q_1\overline{m_1,m_2}$, $m_1,m_2\in N$ 對圖靈機 Z_A 存在著以下算式：

$$\begin{aligned}\alpha_1=q_1\overline{m_1,m_2} &= q_1\overline{m_1}B\overline{m_2}\\ &= q_111^{m_1}B11^{m_2}\\ &\to q_1B1^{m_1}B11^{m_2}\\ &\to Bq_21^{m_1}B11^{m_2}\\ &\to \cdots\cdots\\ &\to B1^{m_1}q_2B11^{m_2}\\ &\to B1^{m_1}Bq_311^{m_2}\\ &\to B1^{m_1}Bq_3B1^{m_2}=\mathrm{Res}_{Z_A}(\alpha_1).\end{aligned}$$

因為

$$A(m_1,m_2)=m_1+m_2=\langle B1^{m_1}Bq_3B1^{m_2}\rangle=\langle\mathrm{Res}_{Z_A}(\alpha_1)\rangle=\psi_{Z_A}^{(2)}(m_1,m_2),$$

所以函數 $A(x,y)=x+y$ 是可計算的。

例題 **1.2** 函數 $S(x)=x+1$ 是可計算的。設圖靈機

$$Z_S=\{q_1S_1S_1q_2\}.$$

表示式 $\alpha_1=q_1\overline{m}$, $m\in N$ 對圖靈機 Z_S 存在著以下算式：

$$\alpha_1=q_1\overline{m}\to q_2\overline{m}=\mathrm{Res}_{Z_S}(\alpha_1).$$

因為

$$S(m)=m+1=\langle q_2\overline{m}\rangle=\langle\mathrm{Res}_{Z_S}(\alpha_1)\rangle=\psi_{Z_S}(m),$$

所以函數 $S(x)=x+1$ 是可計算的。

例題 **1.3** 函數

$$B(x,y) = x \dot{-} y = \begin{cases} x-y, & x \geq y \\ 0, & x < y \end{cases}$$

是可計算的。設圖靈機 Z_B 由以下四元數列所組成：

$$\begin{array}{ll} q_1 1 B q_1, & q_1 B R q_2, \\ q_2 1 R q_2, & q_2 B R q_3, \\ q_3 1 R q_3, & q_3 B L q_4, \\ q_4 1 B q_4, & q_4 B L q_5, \\ q_5 1 L q_6, & q_6 1 L q_6, \\ q_6 B L q_7, & q_7 1 L q_8, \\ q_7 B R q_9, & q_8 1 L q_8, \\ q_8 B R q_1, & q_9 B R q_{10}, \\ q_{10} 1 B q_9. & \end{array}$$

(1) 若 $m_1, m_2 \in N, m_1 \geq m_2, k = m_1 - m_2$，則表示式 $\alpha_1 = q_1 \overline{m_1, m_2}$ 對圖靈機 Z_B 存在著以下算式：

$$\begin{array}{rcl} \alpha_1 & = & q_1 \overline{m_1} B \overline{m_2} \\ & = & q_1 1 1^{m_2} 1^k B 1^{m_2+1} \\ & \to & q_1 B 1^{m_2} 1^k B 1^{m_2+1} \\ & \to & B q_2 1^{m_2} 1^k B 1^{m_2+1} \\ & \to & \cdots \\ & \to & B 1^{m_2} 1^k q_2 B 1^{m_2+1} \\ & \to & B 1^{m_2} 1^k B q_3 1^{m_2+1} \\ & \to & \cdots \\ & \to & B 1^{m_2} 1^k B 1^{m_2} 1 q_3 B \\ & \to & B 1^{m_2} 1^k B 1^{m_2} q_4 1 B \\ & \to & B 1^{m_2} 1^k B 1^{m_2} q_4 B B \\ & \to & \cdots \\ & \to & B 1^{m_2} 1^k B q_6 1^{m_2} B B \\ & \to & B 1^{m_2} 1^k q_6 B 1^{m_2} B B \\ & \to & \cdots \\ & \to & q_8 B 1^{m_2} 1^k B 1^{m_2} B B \\ & \to & B q_1 1^{m_2} 1^k B 1^{m_2} B B = \alpha_s, \end{array}$$

比對 α_s 與 α_1 的差異，並繼續上述的過程，可得到以下結果：

$$\begin{aligned}
\alpha_s &\rightarrow \cdots \\
&\rightarrow B^{m_2}q_1 1 1^k B 1 B^{m_2} B \\
&\rightarrow \cdots \\
&\rightarrow B^{m_2+1}1^k q_2 B 1 B^{m_2} B \\
&\rightarrow \cdots \\
&\rightarrow B^{m_2+1}1^k B q_4 1 B^{m_2} B \\
&\rightarrow B^{m_2+1}1^k B q_4 B B^{m_2} B \\
&\rightarrow B^{m_2+1}1^k q_5 B B B^{m_2} B = \mathrm{Res}_{Z_B}(\alpha_1).
\end{aligned}$$

因此

$$B(m_1, m_2) = m_1 \dot{-} m_2 = m_1 - m_2 = \langle \mathrm{Res}_{Z_B}(\alpha_1) \rangle = \psi^{(2)}_{Z_B}(m_1, m_2).$$

(2) 若 $m_1, m_2 \in N, m_1 < m_2, k' = m_2 - m_1$，則表示式 $\alpha_1 = q_1 \overline{m_1, m_2}$ 對圖靈機 Z_B 存在著以下算式：

$$\begin{aligned}
\alpha_1 &= q_1 1 1^{m_1} B 1^{k'} 1^{m_1+1} \\
&\rightarrow \cdots \\
&\rightarrow B q_1 1^{m_1} B 1^{k'} 1^{m_1} B B \\
&\rightarrow \cdots \\
&\rightarrow B^{m_1} q_1 1 B 1^{k'} 1 B^{m_1} B \\
&\rightarrow B^{m_1} q_1 B B 1^{k'} 1 B^{m_1+1} \\
&\rightarrow B^{m_1} B q_2 B 1^{k'} 1 B^{m_1+1} \\
&\rightarrow B^{m_1} B B q_3 1^{k'} 1 B^{m_1+1} \\
&\rightarrow \cdots \\
&\rightarrow B^{m_1} B B 1^{k'} q_4 1 B^{m_1+1} \\
&\rightarrow B^{m_1} B B 1^{k'} q_4 B B^{m_1+1} \\
&\rightarrow \cdots \\
&\rightarrow B^{m_1} B q_6 B 1^{k'} B B^{m_1+1} \\
&\rightarrow B^{m_1} q_7 B B 1^{k'} B B^{m_1+1} \\
&\rightarrow B^{m_1} B q_9 B 1^{k'} B B^{m_1+1} \\
&\rightarrow B^{m_1} B B q_{10} 1^{k'} B B^{m_1+1} \\
&\rightarrow B^{m_1} B B q_9 B 1^{k'-1} B B^{m_1+1} \\
&\rightarrow B^{m_1} B B B q_{10} 1^{k'-1} B B^{m_1+1} \\
&\rightarrow \cdots \\
&\rightarrow B^{m_1+k'+2} q_{10} B B^{m_1+1} = \mathrm{Res}_{Z_B}(\alpha_1).
\end{aligned}$$

因此

$$B(m_1, m_2) = m_1 \dot{-} m_2 = 0 = \langle \mathrm{Res}_{Z_B}(\alpha_1) \rangle = \psi^{(2)}_{Z_B}(m_1, m_2).$$

由 (1)(2) 的討論我們證明了，對任意兩數 $x, y \in N$ 恆有

$$B(x,y) = x \dot{-} y = \psi^{(2)}_{Z_B}(x,y),$$

所以函數 $B(x,y) = x \dot{-} y$ 是可計算的。

例題 **1.4** 函數 $I(x) = x$ 是可計算的。設圖靈機

$$Z_I = \{q_1 1 B q_1\}.$$

表示式 $\alpha_1 = q_1\overline{n}, n \in N$ 對圖靈機 Z_I 存在著以下算式：

$$\alpha_1 = q_1\overline{n} = q_1 11^n \to q_1 B 1^n.$$

因為

$$I(n) = n = \langle q_1 B 1^n \rangle = \langle \mathrm{Res}_{Z_I}(\alpha_1) \rangle = \psi_{Z_I}(n),$$

所以函數 $I(x) = x$ 是可計算的。

例題 **1.5** 函數 $U^n_i(x_1, \cdots, x_n) = x_i, 1 \le i \le n$ 是可計算的。設圖靈機 Z_U 由以下四元數列所組成：

$$q_j 1 B q_{2n+j},$$
$$q_j B R q_{j+1},$$
$$q_{2n+j} B R q_j,$$
$$q_i 1 B q_i,$$
$$q_i B R q_{2n+i},$$
$$q_{2n+i} 1 R q_{2n+i},$$
$$q_{2n+i} B R q_{i+1}.$$

（其中 j 是任何一個介於 1 與 n 之間的數，且 $j \neq i$）對任意 $m_1, \cdots, m_n \in N$，表示式

$$\alpha_1 = q_1 \overline{m_1, \cdots, m_n}$$

對 Z_U 存在著以下算式：

$$\begin{aligned}
\alpha_1 &\to \cdots \\
&\to B^{m_1+1} B q_2 1^{m_2+1} B \cdots B 1^{m_i+1} B \cdots B 1^{m_n+1} \\
&\to \cdots \\
&\to B^{m_1+1} B B^{m_2+1} B \cdots B q_i 1^{m_i+1} B \cdots B 1^{m_n+1} \\
&\to B^{m_1+1} B B^{m_2+1} B \cdots B q_i B 1^{m_i} B \cdots B 1^{m_n+1} \\
&\to B^{m_1+1} B B^{m_2+1} B \cdots B B q_{2n+i} 1^{m_i} B \cdots B 1^{m_n+1} \\
&\to \cdots \\
&\to B^{m_1+1} B B^{m_2+1} B \cdots B 1^{m_i} B q_{i+1} \cdots B 1^{m_n+1} \\
&\to \cdots \\
&\to B^s 1^{m_i} B^t q_n 1^{m_n+1} \quad (s,t\text{代表適當的數}) \\
&\to \cdots \\
&\to B^s 1^{m_i} B^t B^{m_n+1} B q_{n+1} B = \mathrm{Res}_{Z_U}(\alpha_1)
\end{aligned}$$

因為

$$U_i^n(m_1,\cdots,m_n)=m_i=\langle \mathrm{Res}_Z(\alpha_1)\rangle=\psi_Z^{(n)}(m_1,\cdots,m_n).$$

所以函數 $U_i^n(x_1,\cdots,x_n)=x_i$ 是可計算的。

例題 **1.6** 函數 $D'(x,y)=(x+1)(y+1)$ 是可計算的。設圖靈機 $Z_{D'}$ 由以下四元數列所組成：

$$\begin{array}{rr}
q_1 1 B q_1, & q_1 B R q_2,\\
q_2 1 \epsilon q_3, & q_3 \epsilon R q_3,\\
q_3 1 R q_3, & q_3 B R q_4,\\
q_4 1 R q_3, & q_4 B L q_5,\\
q_5 1 L q_6, & q_5 B L q_6,\\
q_6 1 \eta q_6, & q_6 \eta R q_7,\\
q_6 B B q_{10}, & q_7 1 R q_7,\\
q_7 B R q_8, & q_8 1 R q_8,\\
q_8 B 1 q_9, & q_9 1 L q_9,\\
q_9 B L q_9, & q_9 \eta 1 q_5,\\
q_{10} 1 L q_{10}, & q_{10} B L q_{10},\\
q_{10} \epsilon B q_1. &
\end{array}$$

（其中 ϵ,η 代表兩個不為 $1,B$ 且不相同的 S-元素。）對任意 $m_1,m_2\in N$，表示式

$$\alpha_1=q_1\overline{m_1,m_2}=q_1 1^{m_1+1}B1^{m_2+1}$$

對圖靈機 $Z_{D'}$ 存在著以下算式：

$$\begin{aligned}
\alpha_1 &\to q_1 B 1^{m_1} B 1^{m_2+1} \\
&\to B q_2 1^{m_1} B 1^{m_2+1} \\
&\to B q_3 \epsilon 1^{m_{1-1}} B 1^{m_2+1} \\
&\to \cdots \\
&\to B \epsilon 1^{m_1-1} q_3 B 1^{m_2+1} \\
&\to B \epsilon 1^{m_1-1} B q_4 1^{m_2+1} \\
&\to \cdots \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2+1} q_3 B \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2+1} B q_4 B \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2+1} q_5 B B \\
&\to \cdots \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} q_6 1 B B \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} q_6 \eta B B \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} \eta q_7 B B \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} \eta B q_8 B \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} \eta B q_9 1 \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} \eta q_9 B 1 \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} q_9 \eta B 1 \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2} q_5 1 B 1 \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2-1} q_6 1 1 B 1 \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2-1} q_6 \eta 1 B 1 \\
&\to \cdots \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2-1} \eta 1 B 1 q_8 B \\
&\to B \epsilon 1^{m_1-1} B 1^{m_2-1} \eta 1 B 1 q_9 1 \\
&\to \cdots \\
&\to B \epsilon 1^{m_1-1} B \eta 1^{m_2} B 1^{m_2} q_9 1 \\
&\to \cdots \\
&\to B \epsilon 1^{m_1-1} B q_9 \eta 1^{m_2} B 1^{m_2+1} \\
&\to B \epsilon 1^{m_1-1} B q_5 1^{m_2+1} B 1^{m_2+1} \\
&\to B \epsilon 1^{m_1-1} q_6 B 1^{m_2+1} B 1^{m_2+1} \\
&\to B \epsilon 1^{m_1-1} q_{10} B 1^{m_2+1} B 1^{m_2+1} \\
&\to \cdots \\
&\to B q_{10} \epsilon 1^{m_1-1} B 1^{m_2+1} B 1^{m_2+1} \\
&\to B q_1 B 1^{m_1-1} B 1^{m_2+1} B 1^{m_2+1} \\
&\to B B q_2 1^{m_1-1} B 1^{m_2+1} B 1^{m_2+1} = \alpha_k,
\end{aligned}$$

上述的過程中，我們發現當 1^{m_1} 少了一個 1，就會多了一組 1^{m_2+1}，因此繼續

這個算式可得到以下結果：

$$\begin{aligned}\alpha_k &\to \cdots \\ &\to B^{m_1}q_{10}\epsilon B1^{m_2+1}B1^{m_2+1}B\cdots B1^{m_2+1} \\ &\quad (\text{重覆}m_1+1\text{次的}B1^{m_2+1}) \\ &\to \cdots \\ &\to B^{m_1+1}q_2B1^{m_2+1}B1^{m_2+1}B\cdots B1^{m_2+1} = \mathrm{Res}_{Z_{D'}}(\alpha_1).\end{aligned}$$

因為

$$D'(m_1,m_2) = (m_1+1)(m_2+1) = \langle \mathrm{Res}_{Z_{D'}}(\alpha_1)\rangle = \psi^{(2)}_{Z_{D'}}(m_1,m_2),$$

所以函數 $D'(x,y) = (x+1)(y+1)$ 是可計算的。

例題 **1.7** 函數 $C(x) = 1$ 是可計算的。令圖靈機

$$Z_C = \{q_1 1Bq_1, q_1BBq_2, q_2BRq_3, q_3 1Bq_2, q_3B1q_2\}.$$

表示式 $\alpha_1 = q_1\overline{m}, m \in N$ 對圖靈機 Z_C 存在著以下算式：

$$\begin{aligned}\alpha_1 &\to q_1B1^m \\ &\to q_2B1^m \\ &\to Bq_3 1^m \\ &\to Bq_2B1^{m-1} \\ &\to \cdots\cdots \\ &\to B^m q_2 B \\ &\to B^{m+1}q_3B \\ &\to B^{m+1}q_2 1 = \mathrm{Res}_{Z_C}(\alpha_1),\end{aligned}$$

因為

$$C(m) = 1 = \langle B^{m+1}q_2 1\rangle = \langle \mathrm{Res}_{Z_C}(\alpha_1)\rangle = \psi_{Z_C}(m).$$

所以函數 $C(x) = 1$ 是可計算的。

1.3 基本引理

定義 **1.6** 設 Z 是一個圖靈機，符號 $Z^{(n)}$ 代表以 q_{n+i} 取代 Z 中所有 q_i 所生成的新圖靈機；符號 $\theta(Z)$ 代表 Z 所有 q-元素中最大的足碼 i。

由定義 1.3 我們知道，符號 $\langle M\rangle$ 代表 1 在表示式 M 中出現的次數，其值與元素 B 無關，而算式中每個表示式最前與最後的 B-數列（元素 B 所構成的有限數列）並不會影響終結式 1 出現的次數，因此我們常將位在表示式最前與最後的 B-數列省略不記。例如：表示式 $BBS_3BS_2q_3B1S_3BBBB$ 常記作 $S_3BS_2q_3B1S_3$。

定義 **1.7** 設 Z 是一個圖靈機，若 Z 不包含以 $q_{\theta(Z)}$ 為首的四元數列且當 $\mathrm{Res}_Z(q_1\overline{m_1,\cdots,m_n}), m_1,\cdots,m_n \in N$ 有定義時，可找到 $r_1,\ldots,r_s \in N$ 使得

$$\mathrm{Res}_Z(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Z)}\overline{r_1,\cdots,r_s},$$

(表示式最後的 B-數列省略不記) 我們就稱 Z 是一個 n-正則圖靈機，或稱圖零機 Z 是 n-正則的。

引理 **1.1** 設 Z 是一個圖靈機，對任意正整數 n，存在一個 n-正則圖靈機 Z'，使得當 $\mathrm{Res}_Z(q_1\overline{m_1,\cdots,m_n})$ 有定義時，

$$\mathrm{Res}_{Z'}(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Z')}\overline{\psi_Z^{(n)}(m_1,\cdots,m_n)}.$$

〔證明〕令 λ,σ 代表兩個相異且不為 $1, B$，亦不屬於 Z 的 S-元素。令圖靈機 Z_1 是由以下四元數列所組成：

$$\begin{array}{ll} q_1 1 L q_1, & q_1 B \lambda q_1, \\ q_1 \lambda R q_2, & q_2 1 R q_2, \\ q_2 B R q_3, & q_3 1 R q_2, \\ q_3 B L q_4, & q_4 B \sigma q_4, \\ q_4 \sigma L q_5, & q_5 1 L q_5, \\ q_5 B L q_5, & q_5 \lambda R q_6. \end{array}$$

表示式 $\alpha_1 = q_1\overline{m_1,\cdots,m_n}$ 對 Z_1 存在著以下算式：

$$\begin{array}{rcl} \alpha_1 & \to & \cdots \\ & \to & \lambda q_2 \overline{m_1} B \cdots B \overline{m_n} \\ & \to & \cdots \\ & \to & \lambda \overline{m_1} B \overline{m_2} \cdots B \overline{m_n} q_2 B \\ & \to & \cdots \\ & \to & \lambda B \cdots B \overline{m_n} q_4 \sigma B \\ & \to & \cdots \\ & \to & \lambda q_5 \overline{m_1} B \cdots B \overline{m_n} \sigma B \\ & \to & \cdots \\ & \to & \lambda q_6 (\overline{m_1,\cdots,m_n}) \sigma B \\ & = & \alpha_r = \mathrm{Res}_{Z_1}(\alpha_1). \end{array}$$

令圖靈機 Z_2 是由 $Z^{(5)}$ 及下列四元數列所組成：

$$q_i \lambda B q_{K+i},$$

$$q_{K+i} B L q_{2K+i},$$

$$q_{2K+i} B \lambda q_{2K+i},$$

$$q_{2K+i} \lambda R q_i,$$

$$q_i\sigma Bq_{3K+i},$$
$$q_{3K+i}BRq_{4K+i},$$
$$q_{4K+i}B\sigma q_{4K+i},$$
$$q_{4K+i}\sigma Lq_i.$$

（其中 q_i 是 $Z^{(5)}$ 的任何一個 q-元素，且 $K=\theta(Z^{(5)})$）對任意 S-數列 P_0,Q_0，表示式 $q_i\lambda P_0,Q_0q_j\sigma$ 對 Z_2 存在著以下算式：

$$\begin{aligned} q_i\lambda P_0 &\to q_{K+i}BP_0\\ &\to q_{2K+i}BBP_0\\ &\to q_{2K+i}\lambda BP_0\\ &\to \lambda q_iBP_0, \end{aligned}$$

$$\begin{aligned} Q_0q_j\sigma &\to Q_0q_{3K+j}B\\ &\to Q_0Bq_{4K+j}B\\ &\to Q_0Bq_{4K+j}\sigma\\ &\to Q_0q_jB\sigma. \end{aligned}$$

因此當 $\mathrm{Res}_Z(\alpha_1)$ 有定義時，表示式 $\alpha_r=\lambda q_6\overline{m_1,\cdots,m_n}\sigma B$ 對 Z_2 存在著算式：

$$\alpha_r=\lambda q_6(\overline{m_1,\cdots,m_n})\sigma B\to\lambda\alpha\sigma B=\mathrm{Res}_{Z_2}(\alpha_r).$$

其中表示式

$$\alpha=\mathrm{Res}_{Z^{(5)}}(q_6\overline{m_1,\cdots,m_n}).$$

令 $L=5K+1$，令圖靈機 Z_3 由以下四元數列所組成：

$$q_iS_jS_jq_L,$$

其中 q_i 是 Z_2 中任何一個 q-元素，S_i 是 Z_2 中任何一個 S-元素，但 q_iS_j 不可與 Z_2 中任一個四元數列前兩個元素相同。令表示式 $\lambda\alpha\sigma B=\lambda Pq_iQ\sigma B$ (P,Q 為適當的 S-數列）我們得到一個算式：

$$\lambda Pq_iQ\sigma B\to\lambda Pq_LQ\sigma B=\mathrm{Res}_{Z_3}(\lambda\alpha\sigma B).$$

令圖靈機 Z_4 由以下四元數列所組成，其中 S 代表 Z 中任何一個不為 $1,B$ 的 S-元素。

$$\begin{aligned} q_L1Lq_L,&\quad q_LBLq_L,\\ q_LSLq_L,&\quad q_L\lambda Rq_{L+1},\\ q_{L+1}SBq_{L+1},&\quad q_{L+1}BRq_{L+1},\\ q_{L+1}1Bq_{L+2},&\quad q_{L+1}\sigma Bq_{L+4},\\ q_{L+2}BLq_{L+2},&\quad q_{L+2}1Rq_{L+3},\\ q_{L+2}\lambda Rq_{L+3},&\quad q_{L+3}B1q_{L+3},\\ q_{L+3}1Rq_{L+1},&\quad q_{L+4}BLq_{L+4},\\ q_{L+4}1Lq_{L+4},&\quad q_{L+4}\lambda 1q_{L+5}. \end{aligned}$$

對 Z_4 可得到一個算式：

$$\begin{aligned}
\lambda P q_L Q\sigma B &\to \cdots \\
&\to q_L\lambda PQ\sigma B \\
&\to \lambda q_{L+1} PQ\sigma B \\
&\to \cdots \\
&\to \lambda B^s q_{L+1} 1 M\sigma B \\
&\quad (M\text{代表適當的}S\text{-數列}, s\text{代表適當的數}) \\
&\to \lambda B^s q_{L+2} B M\sigma B \\
&\to \cdots \\
&\to q_{L+2}\lambda B^{s+1} M\sigma B \\
&\to \lambda q_{L+3} B^{s+1} M\sigma B \\
&\to \lambda q_{L+3} 1 B^s M\sigma B \\
&\to \lambda 1 q_{L+1} B^s M\sigma B \\
&\to \cdots \\
&\to \lambda 1^p B^t q_{L+1}\sigma B \\
&\quad (p = \langle \lambda P q_i Q\sigma B\rangle, t\text{代表適當的數}) \\
&\to \lambda 1^p B^t q_{L+4} BB \\
&\to \cdots \\
&\to q_{L+4}\lambda 1^p \\
&\quad (\text{最後的}B\text{-數列省略}) \\
&\to q_{L+5} 1^{p+1}.
\end{aligned}$$

令 $Z' = Z_1 \bigcup Z_2 \bigcup Z_3 \bigcup Z_4$，則

$$\begin{aligned}
\mathrm{Res}_{Z'}(\alpha_1) &= q_{L+5} 1^{p+1} \\
&= q_{L+5} 1^{\langle \mathrm{Res}_Z(q_1 \overline{m_1,\cdots,m_n})\rangle + 1} \\
&= q_{\theta(Z')} \overline{\psi_Z^{(n)}(m_1,\cdots,m_n)}.
\end{aligned}$$

又因為圖靈機 Z' 不包括以 $\theta(Z') = L+5$ 為首的四元數列，所以 Z' 是 n-正則的。 ⊠

引理 **1.2** 設 Z 是一個 n-正則圖靈機，若

$$\mathrm{Res}_Z(q_1 \overline{m_1,\ldots,m_n}) = q_{\theta(Z)} \overline{r_1,\cdots,r_s},$$

則對任意正整數 p，存在一個 $(p+n)$-正則圖靈機 Z_p 使得

$$\mathrm{Res}_{Z_p}(q_1 \overline{k_1,\cdots,k_p,m_1,\cdots,m_n}) = q_{\theta(Z_p)} \overline{k_1,\cdots,k_p,r_1,\cdots,r_s}.$$

若 $\mathrm{Res}_Z(q_1 \overline{m_1,\cdots,m_n})$ 未定義，則

$$\mathrm{Res}_{Z_p}(q_1 \overline{k_1,\cdots,k_p,m_1,\cdots,m_n})$$

也未定義。

〔證明〕令 δ,ϵ 代表兩個相異且不為 $1, B$、亦不屬於 Z 的 S-元素。令圖靈機 U_1 是由以下四元數列所組成：

$$\begin{aligned}
q_1 1\delta q_1, &\qquad q_1\delta R q_2,\\
q_i 1\epsilon q_i, &\qquad q_i\epsilon R q_i,\\
q_i BR q_{i+1}, &\qquad q_{p+1}1\epsilon q_{p+1},\\
q_{p+1}\epsilon R q_{p+1}, &\qquad q_{p+1}B\epsilon q_{p+2},\\
q_{p+2}\epsilon R q_{p+3}, &
\end{aligned}$$

其中 $2 \le i \le n$。表示式 $\alpha_1 = q_1\overline{k_1, \cdots, k_p, m_1, \cdots, m_n}$ 對圖靈機 U_1 存在著以下算式：

$$\begin{aligned}
\alpha_1 &\to q_1\delta 1^{k_1}B1^{k_2+1}B\cdots B1^{k_p+1}B\overline{m_1, \cdots, m_n}\\
&\to \delta q_2 1^{k_1}B1^{k_2+1}B\cdots B1^{k_p+1}B\overline{m_1, \cdots, m_n}\\
&\to \cdots\\
&\to \delta\epsilon^{k_1}B\epsilon^{k_2+1}\cdots B\epsilon^{k_p+1}q_{p+1}B\overline{m_1, \cdots, m_n}\\
&\to \delta\epsilon^{k_1}B\epsilon^{k_2+1}\cdots B\epsilon^{k_p+1}q_{p+2}\epsilon\overline{m_1, \cdots, m_n}\\
&\to \delta\epsilon^{k_1}B\epsilon^{k_2+1}\cdots B\epsilon^{k_p+1}\epsilon q_{p+3}\overline{m_1, \cdots, m_n}\\
&= \alpha_r = \mathrm{Res}_{U_1}(\alpha_1).
\end{aligned}$$

令 $N = \theta(Z^{(p+2)})$，令圖靈機 U_2 是由 $Z^{(p+2)}$ 與以下四元數列所組成：

$$\begin{aligned}
q_i\epsilon 1 q_{N+i}, &\qquad q_{N+i}1Lq_{N+i},\\
q_{N+i}\epsilon Lq_{N+i}, &\qquad q_{N+i}BLq_{N+i},\\
q_{N+i}\delta Bq_{2N+i}, &\qquad q_{2N+i}BLq_{3N+i},\\
q_{3N+i}B\delta q_{3N+i}, &\qquad q_{3N+i}\delta Rq_{4N+i},\\
q_{4N+i}\epsilon Rq_{5N+i}, &\qquad q_{4N+i}BRq_{5N+i},\\
q_{5N+i}\epsilon Lq_{6N+i}, &\qquad q_{5N+i}BLq_{7N+i},\\
q_{5N+i}1Bq_i, &\qquad q_{6N+i}\epsilon\epsilon q_{8N+i},\\
q_{6N+i}B\epsilon q_{8N+i}, &\qquad q_{7N+i}\epsilon Bq_{8N+i},\\
q_{7N+i}BBq_{8N+i}, &\qquad q_{8N+i}\epsilon Rq_{4N+i},\\
q_{8N+i}BRq_{4N+i}. &
\end{aligned}$$

其中 q_i 是 $Z^{(p+2)}$ 中任何一個 q-元素。設 P 是一個 S-數列，對圖靈機 U_2 存在

以下算式：

$$\begin{aligned}
& \delta\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_{p+1}}q_i\epsilon P \\
\to\ & \delta\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}q_{N+i}1P \\
\to\ & \cdots \\
\to\ & q_{N+i}\delta\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}1P \\
\to\ & q_{2N+i}B\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}1P \\
\to\ & q_{3N+i}BB\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}1P \\
\to\ & q_{3N+i}\delta B\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}1P \\
\to\ & \delta q_{4N+i}B\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}1P \\
\to\ & \delta Bq_{5N+i}\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}1P \\
\to\ & \cdots \\
\to\ & \delta\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}\epsilon q_{5N+i}1P \\
\to\ & \delta\epsilon^{k_1}B\epsilon^{k_2+1}B\cdots B\epsilon^{k_p+1}\epsilon q_iBP
\end{aligned}$$

令 $U_3 = U_1 \bigcup U_2$，若 $\mathrm{Res}_Z(q_1\overline{m_1,\cdots,m_n})$ 有定義，則表示式 α_1 對 U_3 存在著以下算式：

$$\begin{aligned}
\alpha_1 \ \to\ & \cdots \\
\to\ & \delta\epsilon^{k_1}B\cdots B\epsilon^{k_p+1}\epsilon q_{p+3}\overline{m_1,\cdots,m_n} = \alpha_r \\
\to\ & \cdots \\
\to\ & \delta\epsilon^{k_1}B\cdots B\epsilon^{k_p+1}\epsilon q_N\overline{r_1,\cdots,r_s}.
\end{aligned}$$

令 $L = \theta(U_3)$，令圖靈機 Z_p 是由 U_3 及下列四元數列所組成：

$$q_N1Lq_N,$$

$$q_N\epsilon Bq_{L+1},$$

$$q_{L+1}BLq_{L+1},$$

$$q_{L+1}\epsilon 1q_{L+1},$$

$$q_{L+1}1Lq_{L+1},$$

$$q_{L+1}\delta 1q_{L+2}.$$

我們可得到以下算式：

$$\begin{aligned}
\alpha_1 \ \to\ & \cdots \\
\to\ & \delta\epsilon^{k_1}B\cdots B\epsilon^{k_p+1}\epsilon q_N\overline{r_1,\cdots,r_s} = \mathrm{Res}_{U_3}(\alpha_1) \\
\to\ & \delta\epsilon^{k_1}B\cdots B\epsilon^{k_p+1}q_N\epsilon\overline{r_1,\cdots,r_s} \\
\to\ & \delta\epsilon^{k_1}B\cdots B\epsilon^{k_p+1}q_{L+1}B\overline{r_1,\cdots,r_s} \\
\to\ & \cdots \\
\to\ & q_{L+2}1^{k_1+1}B\cdots B1^{k_p+1}B\overline{r_1,\cdots,r_s} \\
=\ & q_{\theta(Z_p)}\overline{k_1,\cdots,k_p,r_1,\cdots,r_s},
\end{aligned}$$

使得

$$\mathrm{Res}_{Z_p}(q_1\overline{k_1,\cdots,k_p,m_1,\cdots,m_n}) = q_{\theta(Z_p)}\overline{k_1,\cdots,k_p,r_1,\cdots,r_s}.$$

若 $\mathrm{Res}_z(q_1\overline{m_1,\cdots,m_n})$ 未定義，則 $\mathrm{Res}_{U_3}(\alpha_1)$ 未定義，$\mathrm{Res}_{Z_p}(\alpha_1)$ 也未定義。 ⊠

引理 **1.3** 設 $n,p\in N, n>0, p\geq 0$，存在一個 $(p+n)$-正則圖靈機 C_p，使得對任意 $k_1,\cdots,k_p,m_1,\cdots,m_n\in N$,

$$\mathrm{Res}_{C_p}(q_1\overline{k_1,\cdots,k_p,m_1,\cdots,m_n}) = q_{p+16}\overline{m_1,\cdots,m_n,k_1,\cdots,k_p,m_1,\cdots,m_n}.$$

〔證明〕令圖靈機 C_p 是由以下四元數列所組成：

$$\begin{array}{rr}
q_1 1 L q_1, & q_1 B L q_2,\\
q_2 B \lambda q_2, & q_2 \lambda R q_3,\\
q_i 1 R q_i, & q_i B R q_{i+1},\\
q_{p+3} 1 R q_{p+3}, & q_{p+3} B \sigma q_{p+3},\\
q_{p+3}\sigma R q_{p+4}, & q_{p+4} 1 R q_{p+4},\\
q_{p+4} B R q_{p+5}, & q_{p+5} 1 R q_{p+4},\\
q_{p+5} B L q_{p+6}, & q_{p+6} 1 L q_{p+7},\\
q_{p+6} B L q_{p+7}, & q_{p+7} 1 \omega q_{p+7},\\
q_{p+7}\omega L q_{p+8}, & q_{p+7} B \beta q_{p+7},\\
q_{p+7}\beta L q_{p+11}, & q_{p+7}\sigma B q_{p+15},\\
q_{p+8} 1 L q_{p+8}, & q_{p+8} B L q_{p+8},\\
q_{p+8}\sigma L q_{p+8}, & q_{p+8}\lambda\omega q_{p+10},\\
q_{p+8}\omega 1 q_{p+9}, & q_{p+8}\beta B q_{p+9},\\
q_{p+9} 1 L q_{p+10}, & q_{p+9} B L q_{p+10},\\
q_{p+10} B\omega q_{p+10}, & q_{p+10}\omega R q_{p+14},\\
q_{p+11} 1 L q_{p+11}, & q_{p+11} B L q_{p+11},\\
q_{p+11}\sigma L q_{p+11}, & q_{p+11}\omega 1 q_{p+12},\\
q_{p+11}\beta B q_{p+12}, & q_{p+12} 1 L q_{p+13},\\
q_{p+12} B L q_{p+13}, & q_{p+13} B \beta q_{p+13},\\
q_{p+13}\beta R q_{p+14}, & q_{p+14} 1 R q_{p+14},\\
q_{p+14} B R q_{p+14}, & q_{p+14}\sigma R q_{p+14},\\
q_{p+14}\omega 1 q_{p+6}, & q_{p+14}\beta B q_{p+6},\\
q_{p+15} 1 L q_{p+15}, & q_{p+15} B L q_{p+15},\\
q_{p+15}\omega 1 q_{p+16}, &
\end{array}$$

其中 $3\leq i\leq p-2$。若 $p=0$，表示式 $\alpha_1 = q_1\overline{m_1,\cdots,m_n}$ 對圖靈機 C_0 存在著

以下算式：

$$\begin{aligned}
\alpha_1 &\to \cdots \\
&\to q_2\lambda B\overline{m_1,\cdots,m_n} \\
&\to \lambda q_3 B\overline{m_1,\cdots,m_n} \\
&\to \lambda q_3\sigma\overline{m_1,\cdots,m_n} \\
&\to \cdots \\
&\to \lambda\sigma\overline{m_1,\cdots,m_{n-1}}B1^{m_n}q_7 1 \\
&\to \cdots \\
&\to q_8\lambda\sigma\overline{m_1,\cdots,m_{n-1}}B1^{m_n}\omega \\
&\to q_{10}\omega\sigma\overline{m_1,\cdots,m_{n-1}}B1^{m_n}\omega \\
&\to \cdots \\
&\to \omega\sigma\overline{m_1,\cdots,m_{n-1}}B1^{m_n}q_{14}\omega \\
&\to \cdots \\
&\to q_{11}\omega 1^{m_n}\sigma\overline{m_1,\cdots,m_{n-1}}\beta 1^{m_n+1} \\
&\to q_{12}1^{m_n+1}\sigma\overline{m_1,\cdots,m_{n-1}}\beta 1^{m_n+1} \\
&\to \cdots \\
&\to q_{13}B1^{m_n+1}\sigma\overline{m_1,\cdots,m_{n-1}}B1^{m_n+1} \\
&\to \cdots \\
&\to \omega 1^{m_1}B\overline{m_2,\cdots,m_n}q_7\sigma\overline{m_1,\cdots,m_n} \\
&\to q_{15}\omega 1^{m_1}B\overline{m_2,\cdots,m_n}B\overline{m_1,\cdots,m_n} \\
&\to q_{16}\overline{m_1,\cdots,m_n,m_1,\cdots,m_n}.
\end{aligned}$$

使得

$$\mathrm{Res}_{C_0}(\alpha_1) = q_{16}\overline{m_1,\cdots,m_n,m_1,\cdots,m_n}.$$

若 $p>0$，則表示式 $\alpha_1 = q_1\overline{k_1,\cdots,k_p,m_1,\cdots,m_n}$ 對圖靈機 C_p 存在著以下算式：

$$\begin{aligned}
q_1\overline{k_1,\cdots,k_p,m_1,\cdots,m_n} &\to \cdots \\
&\to q_2\lambda B\overline{k_1,\cdots,k_p,m_1,\cdots,m_n} \\
&\to \cdots \\
&\to \lambda B\overline{k_1,\cdots,k_p}q_{p+3}\sigma\overline{m_1,\cdots,m_n} \\
&\to \cdots \quad (\text{其算法類似} p=0 \text{的情況}) \\
&\to q_{16}\overline{m_1,\cdots,m_n,k_1,\cdots,k_p,m_1,\cdots,m_n}.
\end{aligned}$$

所以

$$\mathrm{Res}_{C_p}(q_1\overline{k_1,\cdots,k_p,m_1,\cdots,m_n}) = q_{16}\overline{m_1,\cdots,m_n,k_1,\cdots,k_p,m_1,\cdots,m_n}.$$

⊠

引理 **1.4** 設 $n,p \in N, n>0, p>0$，存在一個 $(p+n)$-正則圖靈機 R_p，使得對任意 $k_1,\cdots,k_p,m_1,\cdots,m_2 \in N$

$$\mathrm{Res}_{R_p}(q_1\overline{k_1,\cdots,k_p,m_1,\cdots,m_n}) = q_{p+16}\overline{m_1,\cdots,m_n,k_1,\cdots,k_p}.$$

〔證明〕令 R_p 是將圖靈機 C_p 的四元數列

$$q_{p+14}\omega 1 q_{p+6}$$

以

$$q_{p+14}\omega B q_{p+6}$$

取代所構成的新圖靈機。R_p 的算式與 C_p 相似，在 C_p 的算式中，先以 ω 取代 S-數列 $\overline{m_1,\cdots,m_n}$ 的1，複製之後再將 ω 還原為 1；但 R_p 的算式是最後將 ω 以 B 來取代。其算式的過程在此我們省略不證。 ⊠

引理 **1.5** 對任意 n-正則圖靈機 Z，若

$$\mathrm{Res}_Z(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Z)}\overline{r_1,\cdots,r_s},$$

則存在一個 n-正則圖靈機 Z'，使得

$$\mathrm{Res}_{Z'}(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Z')}\overline{r_1,\cdots,r_s,m_1,\cdots,m_n}.$$

若 $\mathrm{Res}_Z(q_1\overline{m_1,\cdots,m_n})$ 未定義，則 $\mathrm{Res}_{Z'}(q_1\overline{m_1,\cdots,m_n})$ 也未定義。

〔證明〕由引理 1.2 可知，存在一個 $2n$-正則圖靈機 U，使得

$$\mathrm{Res}_U(q_1\overline{m_1,\cdots,m_n,m_1,\cdots,m_n}) = q_{\theta(U)}\overline{m_1,\cdots,m_n,r_1,\cdots,r_s}.$$

令圖靈機

$$Z' = C_0 \bigcup U^{(15)} \bigcup R_n^{(14+\theta(U))}.$$

表示式 $\alpha_1 = q_1\overline{m_1,\cdots,m_n}$ 對圖靈機 C_0 存在著以下算式：

$$\begin{aligned} q_1\overline{m_1,\cdots,m_n} &\to \cdots \\ &\to q_{16}\overline{m_1,\cdots,m_n,m_1,\cdots,m_n} = \alpha_2. \end{aligned}$$

若 $\mathrm{Res}_Z(\alpha_1)$ 有定義，則 α_2 對 $U^{(15)}$ 存在著算式：

$$\alpha_2 \to \cdots \to q_{\theta(U^{(15)})}\overline{m_1,\cdots,m_n,r_1,\cdots,r_s} = \alpha_3.$$

又 α_3 對 $R_n^{(14+\theta(U))}$ 存在著算式：

$$\alpha_3 \to \cdots \to q_{\theta(Z')}\overline{r_1,\cdots,r_s,m_1,\cdots,m_n}.$$

因此

$$\mathrm{Res}_{Z'}(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Z')}\overline{r_1,\cdots,r_s,m_1,\cdots,m_n}.$$

若 $\mathrm{Res}_Z(\alpha_1)$ 未定義，則 $\mathrm{Res}_{U^{(15)}}(\alpha_2)$ 未定義，$\mathrm{Res}_{Z'}(\alpha_1)$ 也未定義。 ⊠

引理 **1.6** 設 $Z_1,\cdots,Z_p$ 是 p 個圖靈機， n 是一個正整數，存在一個 n-正則圖靈機 Z'，使得

$$\mathrm{Res}_{Z'}(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Z')}\overline{\psi^{(n)}_{Z_1}(m_1,\cdots,m_n),\cdots,\psi^{(n)}_{Z_p}(m_1,\cdots,m_n)}.$$

〔證明〕利用歸納法。當 $p=1$ 時，顯然成立（由引理 1.1 即可證得）。設 $p=k$ 時成立，我們將證明 $p=k+1$ 時亦成立。若 $Z_1,\cdots,Z_{k+1}$ 是 $k+1$ 個圖靈機，且

$$r_i = \psi^{(n)}_{Z_i}(m_1,\cdots,m_n), \quad 1\le i\le k+1$$

由假設可知，存在一個 n-正則圖靈機 Y_1 使得

$$\mathrm{Res}_{Y_1}(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Y_1)}\overline{r_1,\cdots,r_k}.$$

由引理 1.5 可知，存在一個圖靈機 Y_2，使得

$$\mathrm{Res}_{Y_2}(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Y_2)}\overline{r_1,\cdots,r_k,m_1,\cdots,m_n}.$$

再由引理 1.1 可知，存在一個 n-正則圖靈機 Y_3 使得

$$\mathrm{Res}_{Y_3}(q_1\overline{m_1,\cdots,m_n}) = q_{\theta(Y_3)}\overline{r_{k+1}}.$$

最後由引理 1.2 可知，存在一個 $k+n$-正則圖靈機 Y_4 使得

$$\mathrm{Res}_{Y_4}(q_1\overline{r_1,\cdots,r_k,m_1,\cdots,m_n}) = q_{\theta(Y_4)}\overline{r_1,\cdots,r_k,r_{k+1}}.$$

令 $Z' = Y_2\bigcup Y_4^{(\theta(Y_2)-1)}$，我們可得到以下算式：

$$\begin{aligned} q_1\overline{m_1,\cdots,m_n} &\to \cdots \\ &\to q_{\theta(Y_2)}\overline{r_1,\cdots,r_k,m_1,\cdots,m_n} \\ &\to \cdots \\ &\to q_{\theta(Z')}\overline{r_1,\cdots,r_k,r_{k+1}} = \mathrm{Res}_{Z'}(q_1\overline{m_1,\cdots,m_n}). \end{aligned}$$

所以 $p=k+1$ 時亦成立。 ⊠

1.4 複合運算及最小化運算

定義 **1.8** 若函數 $h(x^{(n)}), f(y^{(m)}), g_1(x^{(n)}),\cdots,g_m(x^{(n)})$ 滿足以下條件：

$$h(x^{(n)}) = f(g_1(x^{(n)}),\cdots,g_m(x^{(n)})),$$

則稱函數 $h(x^{(n)})$ 是由函數 $g_1(x^{(n)}),\cdots,g_m(x^{(n)})$ 透過函數 $f(y^{(m)})$ 複合而成，或稱函數 h 是由函數 $f,g_1,\cdots,g_m$ 的複合運算所生成。函數 h 在 $x^{(n)}$ 有定義僅當函數 $g_1,\cdots,g_m$ 在 $x^{(n)}$ 有定義，且函數 f 在 $(g_1(x^{(n)}),\cdots,g_m(x^{(n)}))$ 有定義。

由定義 1.8 可知，全函數所生成的複合函數也是全函數。

定理 **1.1** 若函數 $f(y^{(m)}), g_1(x^{(n)}), \cdots, g_m(x^{(n)})$ 是可計算的，則它們的複合函數

$$h(x^{(n)}) = f(g_1(x^{(n)}), \cdots, g_m(x^{(n)}))$$

也是可計算的。

〔證明〕因為函數 $g_1(x^{(n)}), \cdots, g_m(x^{(n)})$ 是可計算的，所以存在圖靈機

$$Z_1, \cdots, Z_m$$

使得

$$g_i(x^{(n)}) = \psi^{(n)}_{Z_i}(x^{(n)}), \quad i = 1, \cdots, m$$

由引理 1.6 可知，存在一個 n-正則圖靈機 Z，使得

$$\begin{aligned} \mathrm{Res}_Z(q_1\overline{x^{(n)}}) &= q_{\theta(Z)}\overline{\psi^{(n)}_{Z_1}(x^{(n)}), \cdots, \psi^{(n)}_{Z_m}(x^{(n)})} \\ &= q_{\theta(Z)}\overline{g_1(x^{(n)}), \cdots, g_m(x^{(n)})}. \end{aligned}$$

因為函數 f 是可計算的，所以存在一個圖靈機 Z_f，使得

$$\psi^{(m)}_{Z_f}(y^{(m)}) = f(y^{(m)}).$$

令圖靈機 $Z' = Z \bigcup Z_f^{\theta(Z)-1}$，我們可得到一個算式：

$$\begin{aligned} q_1\overline{x^{(n)}} &\to \cdots \\ &\to q_{\theta(Z)}\overline{g_1(x^{(n)}), \cdots, g_m(x^n)} \\ &\to \cdots \\ &\to \alpha = \mathrm{Res}_{Z_f^{\theta(Z)-1}}(q_\theta\overline{g_1(x^{(n)}), \cdots, g_m(x^{(n)})}). \end{aligned}$$

其中

$$\langle\alpha\rangle = f(g_1(x^{(n)}), \cdots, g_m(x^{(n)})).$$

因為

$$\psi^{(n)}_{Z'}(x^{(n)}) = f(g_1(x^{(n)}), \cdots, g_m(x^{(n)})) = h(x^{(n)}).$$

所以函數 h 是可計算的。 ⊠

例題 **1.8** 函數 $D(x, y) = xy$ 是可計算的。已知函數

$$S(U_2^2(x, y)) = y + 1$$

是由函數 $U_2^2(x, y) = y$ 透過函數 $S(x) = x + 1$ 複合而成的可計算函數。而函數

$$\begin{aligned} h(x, y) &= B(D'(x, y), S(U_2^2(x, y))) \\ &= B((x + 1)(y + 1), y + 1) \\ &= (x + 1)(y + 1) - (y + 1) \\ &= xy + x \end{aligned}$$

是由函數 $D'(x,y), S(U_2^2(x,y))$ 透過函數 $B(x,y)$ 複合而成的可計算函數，所以函數

$$\begin{aligned} D(x,y) &= xy \\ &= (xy+x)\dot{-}x \\ &= B(h(x,y), U_1^2(x,y)). \end{aligned}$$

是由函數 $h(x,y) = xy + x, U_1^2(x,y) = x$ 透過函數 $B(x,y) = x\dot{-}y$ 複合而成的可計算函數。

定義 **1.9** 若函數 $f(y, x^{(n)})$ 對任意 $x^{(n)} \in N^n$，存在一個 $y \in N$ 使得

$$f(y, x^{(n)}) = 0$$

則稱 f 是一個 解析函數。

定義 **1.10** 若函數 $f(y, x^{(n)})$ 是一個解析函數，則函數

$$h(x^{(n)}) = \min_y [f(y, x^{(n)}) = 0]$$

是函數 $f(y, x^{(n)})$ 的最小化函數，或稱函數 h 是由 f 的最小化運算所生成，其函數值是使函數 $f(\overline{y, x^{(n)}})$ 為零的最小值 y。若函數 f 不是一個解析函數，則不存在 f 的最小化函數。

由定義 1.10 可知，最小化運算所生成的函數是全函數。

例題 **1.9** 若函數 $f(y,x) = y - 2x$，則函數 f 是一個解析函數，其生成的最小化函數為

$$h(x) = \min_y [f(y,x)] = 2x.$$

定理 **1.2** 若 $f(y, x^{(n)})$ 是一個可計算的解析函數，則函數 f 的最小化函數

$$h(x^{(n)}) = \min_y [f(y, x^n) = 0],$$

也是可計算的。

〔證明〕令圖靈機

$$U = \{q_1 1 L q_1,\ q_1 B L q_2,\ q_2 B 1 q_3\}.$$

表示式 $\alpha_1 = q_1\overline{x^{(n)}}$ 對圖靈機 U 存在以下算式：

$$\alpha_1 = q_1\overline{x^{(n)}} \to \cdots \to q_3\overline{0, x^{(n)}} = \mathrm{Res}_U(\alpha_1).$$

已知函數 $f(y, x^{(n)})$ 是一個可計算函數，因此存在一個圖靈機 Z_f 使得

$$f(y, x^{(n)}) = \psi_{Z_f}^{(n+1)}(y, x^{(n)}),$$

由引理 1.1 可知，存在一個 $n+1$-正則圖靈機 Y_0，使得

$$\mathrm{Res}_{Y_0}(q_1\overline{y, x^{(n)}}) = q_{\theta(Y_0)}\overline{\psi_{Z_f}}(y, x^{(n)}) = q_{\theta_{Y_0}}\overline{f(y, x^{(n)})}.$$

由引理 1.5 可知：存在一個 $n+1$-正則圖靈機 Y，使得

$$\mathrm{Res}_Y(q_1\overline{y, x^{(n)}}) = q_{\theta(Y)}\overline{f(y, x^{(n)}), y, x^{(n)}}.$$

令 $N = \theta(Y^{(2)})$，則

$$\mathrm{Res}_{Y^{(2)}}(q_3\overline{y, x^{(n)}}) = q_N\overline{f(y, x^{(n)}), y, x^{(n)}}.$$

令圖靈機

$$M = \{q_N 1 B q_N, q_N BRq_{N+1}, q_{N+1}11q_{N+2}, q_{N+1}BRq_{N+4}\}.$$

若 $f(y, x^{(n)}) = k > 0$，對圖靈機 M 存在以下算式：

$$\begin{aligned} q_N\overline{f(y, x^{(n)}), y, x^{(n)}} &= q_N 11^k B\overline{y, x^{(n)}} \\ &\to \cdots \\ &\to Bq_{N+2}1^k B\overline{y, x^{(n)}}. \end{aligned}$$

若 $f(y, x^{(n)}) = 0$，對圖靈機 M 存在以下算式：

$$\begin{aligned} q_N\overline{f(y, x^{(n)}), y, x^{(n)}} &= q_N 1B\overline{y, x^{(n)}} \\ &\to \cdots \\ &\to BBq_{N+4}\overline{y, x^{(n)}}. \end{aligned}$$

令圖靈機

$$Q = \{q_{N+2}1Bq_{N+3}, q_{N+2}B1q_3, q_{N+3}BRq_{N+2}\}.$$

對 Q 存在以下算式：

$$\begin{aligned} q_{N+2}1^k B\overline{y, x^{(n)}} &\to \cdots \\ &\to B^{k+1}q_3\overline{y+1, x^{(n)}}. \end{aligned}$$

由例題 1.5 可知，可計算函數 $U_1^{n+1}(y, x^{(n)}) = y$ 存在一個圖靈機 Z_U 使得

$$U_1^{n+1}(y, x^{(n)}) = y = \psi_{Z_U}^{(n+1)}(y, x^{(n)}).$$

又由引理 1.1 可知，存在一個 $n+1$- 正則圖靈機 Z_1 使得

$$\begin{aligned} \mathrm{Res}_{Z_1}(q_1\overline{y, x^{(n)}}) &= q_{\theta(Z_1)}\overline{y} \\ &= q_{\theta(Z_1)}1^{y+1}. \end{aligned}$$

令圖靈機

$$E = Z_1 \bigcup \{q_{\theta(Z_1)}1Bq_{\theta(Z_1)}\}.$$

令 $K = \theta(E^{(N+3)})$，對圖靈機 $E^{(N+3)}$ 存在以下算式：

$$q_{(N+4)}(\overline{y, x^{(n)}}) \to \cdots \to q_K B1^y.$$

最後令圖靈機

$$Z = U \bigcup Y^{(2)} \bigcup M \bigcup Q \bigcup E^{(N+3)}.$$

設 $f(i,x^{(n)})=r_i$ 若 $r_0\neq 0, r_1\neq 0,\cdots,r_{k-1}\neq 0, r_k=0$，對圖靈機 Z 存在以下算式：

$$\begin{aligned}
q_1\overline{x^{(n)}} &\to \cdots\\
&\to q_3\overline{0,x^{(n)}}=\mathrm{Res}_U(q_1\overline{x^{(n)}})\\
&\to \cdots\\
&\to q_N(\overline{r_0,0,x^{(n)}})=\mathrm{Res}_{Y^{(2)}}(q_3\overline{0,x^{(n)}})\\
&\to \cdots\\
&\to q_{N+2}\overline{r_0-1,0,x^{(n)}}=\mathrm{Res}_M(q_N\overline{r_0,0,x^{(n)}})\\
&\to \cdots\\
&\to q_3\overline{1,x^{(n)}}=\mathrm{Res}_Q(q_{N+2}\overline{r_0-1,0,x^{(n)}})\\
&\to \cdots\\
&\to q_3\overline{k,x^{(n)}}\\
&\to \cdots\\
&\to q_N\overline{r_k,k,x^{(n)}}=\mathrm{Res}_{Y^{(2)}}(q_3\overline{1,x^{(n)}})\\
&= q_N1B\overline{k,x^{(n)}}\\
&\to \cdots\\
&\to q_{N+4}\overline{k,x^{(n)}}=\mathrm{Res}_M(q_N\overline{r_k,k,x^{(n)}})\\
&\to \cdots\\
&\to q_KB1^k=\mathrm{Res}_{E^{(N+3)}}(q_{N+4}\overline{k,x^{(n)}}).
\end{aligned}$$

(算式中表示式最前與最後的 B-數列省略不記) 因為

$$h(x^{(n)})=\min_y[f(y,x^{(n)})=0]=k=\langle q_KB1^k\rangle=\langle\mathrm{Res}_Z(q_1\overline{x}^{(n)})\rangle=\psi_Z^{(n)}(x^{(n)}),$$

所以函數 $h(x^{(n)})$ 是可計算的。 ⊠

第 2 章

遞歸函數 (Recursive Functions)

本章的內容是在討論有名的遞歸函數，並透過（原始）遞歸敘述的相關性質，證出本章最重要的結果：一個函數是可計算函數的充份必要條件為它是一個遞歸函數。

2.1 遞歸函數

在上一章我們曾提到函數：

$$B(x,y) = x\dot{-}y = \begin{cases} x-y, & x \geq y \\ 0, & x < y \end{cases},$$

也提到函數 $f(y, x^{(n)})$ 可生成最小化函數

$$h(x^{(n)}) = \min_y [f(y, x^{(n)}) = 0]$$

的條件為函數 $f(y, x^{(n)})$ 必須是一個解析函數，也就是對任意 $x^{(n)} \in N^n$ 至少存在一個 $y \in N$ 使得 $f(y, x^{(n)}) = 0$。函數值 $h(x^{(n)})$ 是使 $f(y, x^{(n)}) = 0$ 為零的最小值 y，因此最小化函數為全函數。

以下所定義的函數，我們稱為遞歸函數。

定義 **2.1** 若一個函數是由下列的函數開始：

(1) $C(x) = 1$,

(2) $S(x) = x + 1$,

(3) $U_i^n(x_1, \cdots, x_n) = x_i, 1 \leq i \leq n$,

(4) $A(x, y) = x + y$,

(5) $B(x, y) = x\dot{-}y$,

(6) $D(x, y) = xy$,

透過有限次的複合運算、最小化運算所生成，則稱此函數是一個遞歸函數 (recursive function)，或稱這個函數是遞歸的。

已知初始函數

$$C(x) = 1,$$

$$S(x) = x + 1,$$

$$U_i^n(x_1, \cdots, x_n) = x_i, 1 \leq i \leq n,$$

$$A(x, y) = x + y,$$

$$B(x, y) = x \dot{-} y,$$

$$D(x, y) = xy,$$

都是全函數，利用這些函數有限次的複合及最小化運算所生成的函數仍是全函數，所以遞歸函數也是全函數。

由下面這些函數的表示法可看出它們都是遞歸函數。

例題 **2.1** 零函數 $N(x) = 0$ 是遞歸的。因為

$$\begin{aligned} N(x) &= 0 \\ &= x \dot{-} x \\ &= U_1^1(x) \dot{-} U_1^1(x) \\ &= B(U_1^1(x), U_1^1(x)), \end{aligned}$$

所以零函數 $N(x) = 0$ 是由函數 $U_1^1(x)$ 與函數 $U_1^1(x)$ 透過函數 $B(x, y)$ 複合而成的一個遞歸函數。

例題 **2.2** 函數

$$\alpha(x) = 1 \dot{-} x = \begin{cases} 0, & x \neq 0 \\ 1, & x = 0 \end{cases},$$

是遞歸的。因為

$$\begin{aligned} \alpha(x) &= 1 \dot{-} x \\ &= S(N(x)) \dot{-} U_1^1(x) \\ &= B(S(N(x)), U_1^1(x)), \end{aligned}$$

所以函數 $\alpha(x) = 1 \dot{-} x$ 是由函數 $S(N(x))$ 與函數 $U_1^1(x)$ 透過函數 $B(x, y)$ 複合而成的一個遞歸函數。

例題 **2.3** 函數 x^2 是遞歸的。因為

$$\begin{aligned} x^2 &= x \cdot x \\ &= U_1^1(x) \cdot U_1^1(x) \\ &= D(U_1^1(x), U_1^1(x)), \end{aligned}$$

所以函數 x^2 是由函數 $U_1^1(x)$ 與函數 $U_1^1(x)$ 透過函數 $D(x, y)$ 複合而成的一個遞歸函數。

例題 **2.4** 函數 $[\sqrt{x}\,]$（小於或等於 $\sqrt{x}$ 的最大整數）是遞歸的。因為

$$\begin{aligned}[\sqrt{x}\,] &= \min_y[(y+1)^2 \dot{-} x \neq 0] \\ &= \min_y[S(U_2^2(x,y))^2 \dot{-} U_1^2(x,y) \neq 0] \\ &= \min_y[\alpha\left(S(U_2^2(x,y))^2 \dot{-} U_1^2(x,y)\right) = 0],\end{aligned}$$

所以函數 $[\sqrt{x}\,]$ 是由函數 $\alpha\left(S(U_2^2(x,y))^2 \dot{-} U_1^2(x,y)\right)$ 透過最小化運算所生成的一個是遞歸函數。

例題 **2.5** 函數 $|x-y|$ 是遞歸的。因為

$$|x-y| = (x \dot{-} y) + (y \dot{-} x) = A(x \dot{-} y, y \dot{-} x),$$

又因為

$$y \dot{-} x = B(U_2^2(x,y), U_1^2(x,y)),$$

所以函數 $|x-y|$ 是由函數 $B(x,y) = x \dot{-} y$ 與函數 $y \dot{-} x$ 透過函數 $A(x,y)$ 複合而成的一個遞歸函數。

例題 **2.6** 函數

$$[x/y] = \begin{cases} 0, & y = 0 \\ \text{小於或等於 } x/y \text{ 的最大整數}, & y \neq 0 \end{cases}$$

是遞歸的。因為

$$\begin{aligned}[x/y] &= \min_z[y = 0 \bigvee y(z+1) > x] \\ &= \min_z[y = 0 \bigvee y(z+1) \dot{-} x \neq 0] \\ &= \min_z[y = 0 \bigvee \alpha(y(z+1) \dot{-} x) = 0] \\ &= \min_z[y \cdot \alpha(y(z+1) \dot{-} x) = 0].\end{aligned}$$

所以函數 $[x/y]$ 是由函數 $y \cdot \alpha(y(z+1) \dot{-} x)$ 透過最小化運算所生成的一個遞歸函數。

例題 **2.7** 函數

$$R(x,y) = \begin{cases} x, & y = 0 \\ x \text{ 除以 } y \text{ 的餘數}, & y \neq 0 \end{cases}$$

可表示為

$$R(x,y) = x \dot{-} y[x/y].$$

所以函數 $R(x,y)$ 是遞歸的。

定理 **2.1** 遞歸函數是可計算的。

〔證明〕在第一章的例題 $1.7, 1.2, 1.5, 1.1, 1.3, 1.8$ 已經證明了遞歸函數的初始函數：

$$C(x) = 1,$$
$$(x) = x + 1,$$
$$U_i^n(x_1, \cdots, x_n) = x_i, 1 \leq i \leq n,$$
$$A(x, y) = x + y,$$
$$B(x, y) = x \dot{-} y,$$
$$D(x, y) = xy$$

都是可計算的，再由第一章定理 $1.1, 1.2$ 可知：這些函數所生成的複合函數和最小化函數也是可計算的。 ☒

定理 2.1 的逆敘述也是正確的，我們將在本章第二節證明這個結果。

定理 **2.2** 對任意非負整數 x, y, z，存在遞歸函數 $J(x, y), K(z), L(z)$ 使得：

$$\begin{aligned} K(J(x, y)) &= x, \\ L(J(x, y)) &= y, \\ J(K(z), L(z)) &= z. \end{aligned}$$

〔證明〕已知函數

$$J(x, y) = [1 + 2 + \cdots + (x + y)] + x$$

是由 N^2 一對一且映成至 N 的函數。因為

$$[1 + 2 + \cdots + (x + y)] + x = \frac{1}{2}\left((x + y)^2 + 3x + y\right)$$

是非負整數，所以函數

$$\begin{aligned} J(x, y) &= \frac{1}{2}\left((x + y)^2 + 3x + y\right) \\ &= \left[\frac{(x + y)^2 + 3U_1^2(x, y) + U_2^2(x, y)}{S(S(N(U_1^2(x, y))))}\right]. \end{aligned}$$

令函數

$$\begin{aligned} Q_1(z) &= \left[\frac{1}{2}([\sqrt{8z + 1}] + 1)\right] \dot{-} 1 \\ &= [([\sqrt{8z + 1}] + 1)/S(S(N(z)))] \dot{-} 1, \\ Q_2(z) &= 2z \dot{-} (Q_1(z))^2, \\ K(z) &= \left[\frac{1}{2}(Q_2(z) \dot{-} Q_1(z))\right], \\ L(z) &= Q_1(z) \dot{-} K(z). \end{aligned}$$

由以上各函數的表示法可知，函數 $J(x, y), K(z), L(z)$ 都是遞歸函數。

給定非負整數 x, y，設

$$z = J(x, y),$$

我們可推得

$$2z = (x+y)^2 + 3x + y,$$
$$8z + 1 = (2x + 2y + 1)^2 + 8x,$$
$$(2x + 2y + 1)^2 \le 8z + 1 < (2x + 2y + 3)^2,$$
$$2x + 2y + 1 \le \left[\sqrt{8z+1}\right] < 2x + 2y + 3,$$
$$\left[\frac{1}{2}\left([\sqrt{8z+1}] + 1\right)\right] = x + y + 1,$$

因為

$$\begin{aligned} Q_1(z) &= \left[\frac{1}{2}\left([\sqrt{8z+1}] + 1\right)\right] \dot{-} 1 \\ &= (x+y+1)\dot{-}1 = x + y. \\ Q_2(z) &= 2z\dot{-}(Q_1(z))^2 \\ &= ((x+y)^2 + 3x + y)\dot{-}(x+y)^2 = 3x + y. \end{aligned}$$

所以

$$\begin{aligned} K(J(x,y)) &= K(z) \\ &= \left[\frac{1}{2}(Q_2(z)\dot{-}Q_1(z))\right] \\ &= \left[\frac{1}{2}\left((3x+y)\dot{-}(x+y)\right)\right] \\ &= x. \\ L(J(x,y)) &= L(z) \\ &= Q_1(z)\dot{-}K(z) \\ &= (x+y)\dot{-}x \\ &= y. \end{aligned}$$

反之，給定非負整數 z，我們可找到兩個非負整數 x, y，使得 $z = J(x, y)$。因為存在一個非負整數 r，使得

$$0 + 1 + 2 + \cdots + r \le z < 0 + 1 + 2 + \cdots + (r+1).$$

令

$$x = z - (0 + 1 + 2 + \cdots + r) \le r,$$
$$y = r - x,$$

我們可得到

$$\begin{aligned} z &= (1 + 2 + \cdots + (x+y)) + x \\ &= \frac{1}{2}\left((x+y)^2 + 3x + y\right) \\ &= J(x,y). \end{aligned}$$

已知

$$K(z) = x,$$
$$L(z) = y.$$

所以

$$J(K(z), L(z)) = J(x, y) = z.$$

$\boxtimes$

定理 **2.3** 設 $a_0, a_1, a_2, \cdots, a_n$ 是 $n+1$ 個非負整數，則存在非負整數 u, v 使得

$$R(u, 1 + v(i+1)) = a_i.$$

其中

$$\begin{aligned} R(x,y) &= \begin{cases} x, & y = 0, \\ x\text{除以}y\text{的餘數}, & y \neq 0 \end{cases} \\ &= x \dot{-} y[x/y]. \end{aligned}$$

〔證明〕令

$$\begin{aligned} A &= \max\{a_0, a_1, \cdots, a_n\}, \\ v &= 2A \cdot n!, \\ m_i &= 1 + v(i+1). \end{aligned}$$

我們先證明：

$$(m_i, m_j) = 1, 0 \leq i \neq j \leq n.$$

因為 v 可被 $n!$ 整除，所以 $(m_i, n!) = 1$。若

$$d \mid m_i, \quad d \mid m_j, \quad 0 \leq i \neq j \leq n.$$

則

$$d \mid (i+1)m_j - (j+1)m_i = i - j,$$

所以 d 必須是 1，因此 $(m_i, m_j) = 1,$。

最後利用中國剩餘定理可知，存在一個非負整數 u 使得

$$u \equiv a_i \pmod{m_i}, \qquad i = 0, 1, 2, \cdots, n.$$

因為

$$a_i < m_i,$$

所以

$$R(u, 1 + v(i+1)) = R(u, m_i) = R(a_i, m_i) = a_i.$$

$\boxtimes$

定理 **2.4** 設 $a_0, a_1, \cdots, a_n$ 是 $n+1$ 個非負整數，存在遞歸函數 $T(i, w) = T_i(w), 0 \leq i \leq n$ 及非負整數 w_0 使得

$$T(i, w_0) = T_i(w_0) = a_i, \qquad i = 0, 1, 2, \cdots, n.$$

〔證明〕令函數

$$T_i(w) = R\left(K(w), 1 + L(w)(i+1)\right), \quad 0 \le i \le n.$$

由表示法可看出函數 $T_i(w)$ 是遞歸的。在上個定理我們知道存在非負整數 u, v 使得

$$R(u, 1 + v(i+1)) = a_i, \quad i = 0, 1, 2, \cdots, n.$$

取 $w_0 = J(u, v)$，則

$$\begin{aligned} T_i(w_0) &= R\left(K(w_0), 1 + L(w_0)(i+1)\right) \\ &= R\left(K(J(u,v)), 1 + L(J(u,v)(i+1))\right) \\ &= R(u, 1 + v(i+1)) \\ &= a_i, \qquad i = 0, 1, 2, \cdots, n. \end{aligned}$$

⊠

2.2 原始遞歸函數

在第一章介紹了複合運算與最小化運算，在此我們將介紹另一種運算—原始遞歸運算。

定義 **2.2** 若函數 $f(x^{(n)}), g(x^{(n+2)})$ 都是全函數，且函數 $h(x^{(n+1)})$ 滿足：

$$\begin{aligned} h(0, x^{(n)}) &= f(x^{(n)}), \\ h(y+1, x^{(n)}) &= g(y, h(y, x^{(n)}), x^{(n)}), \end{aligned}$$

則稱函數 h 是由函數 f, g 的原始遞歸運算所生成。

定理 **2.5** 若函數 $f(x^{(n)}), g(x^{(n+2)})$ 是遞歸的，則由函數 f, g 的原始遞歸運算所生成的函數 $h(x^{(n+1)})$ 也是遞歸的。

〔證明〕由定理 2.4 可知：給定 $y, x^{(n)}$，對 $y+1$ 個非負整數

$$h(0, x^{(n)}), h(1, x^{(n)}), \cdots, h(y, x^{(n)}),$$

存在遞歸函數 $T_i(w)(i = 0, 1, 2, \cdots, y)$ 及非負整數 w'，使得

$$T_i(w') = h(i, x^{(n)}),$$

設 w_0 是所有可能值 w' 中最小的數。因此

$$\begin{aligned} h(y, x^{(n)}) &= T_y(w_0) \\ &= T_y\left(\min_w \left[(T_0(w) = f(x^{(n)})) \bigwedge \bigwedge_{z=0}^{y-1} (T_{z+1}(w) = g(z, T_z(w), x^{(n)}))\right]\right). \end{aligned}$$

當一個條件對小於等於 $y-1$ 皆成立時，此情況相當於使此條件不成立的最小值為 y，因此上述的表示法等價於

$$\begin{aligned} h(y, x^{(n)}) &= T_y\Big(\min_w \big[(T_0(w) = f(x^{(n)})) \bigwedge \\ &\qquad \{y = \min_z [(T_{z+1}(w) \ne g(z, T_z(w), x^{(n)})) \bigvee (z = y)]\}\big]\Big). \end{aligned}$$

令函數

$$\begin{aligned} H(y,w,x^{(n)}) &= \min_z[T_{z+1}(w) \neq g(z,T_z(w),x^{(n)}) \bigvee (z=y)] \\ &= \min_z[|z-y| \cdot \alpha(|T_{z+1}(w) - g(z,T_z(w),x^{(n)})|) = 0]. \end{aligned}$$

由表示法可知，函數 $H(y,w,x^{(n)})$ 是一個遞歸函數。可將函數 $h(y,x^{(n)})$ 的表示法再改寫成

$$\begin{aligned} h(y,x^{(n)}) &= T_y\left(\min_w\left[T_0(w) = f(x^{(n)})) \bigwedge (y = H(y,w,x^{(n)}))\right]\right) \\ &= T_y\left(\min_w\left[|T_0(w) - f(x^{(n)}| + |y - H(y,w,x^{(n)})| = 0\right]\right). \end{aligned}$$

因此由最終的表示法可直接判斷出函數 $h(y,x^{(n)})$ 是遞歸的。 ⊠

定義 **2.3** 若一個函數是由下列的函數開始：

(1) $C(x) = 1$,

(2) $S(x) = x + 1$,

(3) $N(x) = 0$,

(4) $U_i^n(x_1,\ldots,x_n) = x_i, 1 \leq i \leq n$,

透過有限次的複合及原始遞歸運算所生成，則稱此函數是一個 原始遞歸函數 (primitive recursive function)，或稱這個函數是原始遞歸的。

定理 **2.6** 原始遞歸函數是遞歸的。

〔證明〕由定義 2.1 可知函數 $C(x) = 1, S(x) = x + 1, U_i^n(x_1,\cdots,x_n) = x_i$ 都是遞歸的，再由例題 2.1 可知函數 $N(x) = 0$ 也是遞歸的，因此原始遞歸函數的初始函數都是遞歸的，而遞歸函數有限次的複合運算及原始遞歸運算所生成的函數也是遞歸的。 ⊠

由下面各函數的表示法可看出，它們都是原始遞歸的。

例題 **2.8** 函數 $A(x,y) = x + y$ 是原始遞歸的。因為

$$\begin{aligned} A(0,y) &= y = U_1^1(y) \\ A(x+1,y) &= x + 1 + y \\ &= (x+y) + 1 \\ &= A(x,y) + 1 \\ &= S(U_2^3(x,A(x,y),y)). \end{aligned}$$

所以函數 $A(x,y) = x + y$ 是由函數 $U_1^1(x) = x$ 與函數 $S(U_2^3(x,y,z)) = y + 1$ 的原始遞歸運算所生成的一個原始遞歸函數。

例題 **2.9** 函數 $D(x,y)=xy$ 是原始遞歸的。已知函數 $A(x,y)=x+y$ 是原始遞歸的，所以函數

$$g(u,v,w)=A(U_2^3(u,v,w),U_3^3(u,v,w))=v+w.$$

也是原始遞歸的。又因為

$$\begin{aligned} D(0,y) &= 0=N(y) \\ D(x+1,y) &= xy+y \\ &= D(x,y)+y \\ &= g(x,D(x,y),y). \end{aligned}$$

所以函數 $D(x,y)$ 是由函數 $N(y)=0$ 與函數 $g(u,v,w)=v+w$ 的原始遞歸運算所生成的一個原始遞歸函數。

例題 **2.10** 函數

$$B(x,y)=x\dot{-}y=\begin{cases} x-y, & x\geq y \\ 0, & x<y \end{cases}$$

是原始遞歸的。因為函數

$$P'(x,y)=\begin{cases} 0, & x=0 \\ x\dot{-}1, & x>0 \end{cases}$$

的表示法為

$$\begin{aligned} P'(0,y) &= 0=N(y), \\ P'(x+1,y) &= x=U_1^3(x,P'(x,y),y). \end{aligned}$$

所以函數 $P'(x,y)$ 是原始遞歸的。換言之，函數

$$P(x)=P'(x,x)=\begin{cases} 0, & x=0 \\ x\dot{-}1, & x>0 \end{cases}.$$

也是原始遞歸的。令函數 $B'(y,x)=B(x,y)=x\dot{-}y$，其表示法為

$$\begin{aligned} B'(0,x) &= B(x,0)=x\dot{-}0=x=U_1^1(x), \\ B'(y+1,x) &= B(x,y+1)=x\dot{-}(y+1) \\ &= P(x\dot{-}y)=P(U_2^3(y,B(x,y),x)). \end{aligned}$$

所以函數 $B(x,y)$ 是由函數 $U_1^1(x)=x$ 與函數 $P(U_2^3(x,y,z))$ 的原始遞歸運算所生成的一個原始遞歸函數。

例題 **2.11** 指數函數 $f(x,y)=y^x$ 是原始遞歸的。已知函數 $D(x,y)=xy$ 是一個原始遞歸函數，所以函數

$$g(u,v,w)=D(U_2^3(u,v,w),U_3^3(u,v,w))=v\cdot w$$

也是原始遞歸的。又函數 y^x 的表示法為

$$\begin{aligned} f(0,y) &= y^0=1=S(N(y)) \\ f(x+1,y) &= y^{x+1}=y^x\cdot y=g(x,f(x,y),y), \end{aligned}$$

所以函數 y^x 是由函數 $S(N(y))=1$ 與函數 $g(u,v,w)=v\cdot w$ 的原始遞歸運算所生成的一個原始遞歸函數。

例題 **2.12** 階乘函數 $x!$ 是原始遞歸的。已知函數

$$g(u,v,w) = D(S(U_1^3(u,v,w)), U_2^3(u,v,w)) = D(S(u),v) = (u+1)v$$

是原始遞歸的。而函數 $f(x,y) = x!$ 可表示為

$$\begin{aligned} f(0,y) &= 0! = 1 = S(N(y)). \\ f(x+1,y) &= (x+1)! = (x+1)\cdot x! = g(x, f(x,y), y). \end{aligned}$$

所以函數 $x!$ 是由函數 $S(N(y)) = 1$ 與函數 $g(u,v,w) = (u+1)v$ 的原始遞歸運算所生成的一個原始遞歸函數。

因為函數 $A(x,y) = x+y, B(x,y) = x \dot{-} y, D(x,y) = xy$ 是遞歸的，我們可將遞歸函數的條件修改如下：

定理 **2.7** 一個函數是遞歸的，其充份必要條件為它是由下列的函數開始：

(1) $C(x) = 1$

(2) $S(x) = x+1$

(3) $N(x) = 0$

(4) $U_i^n(x_1,\ldots,x_n) = x_i, 1 \le i \le n$

透過有限次的複合運算、原始遞歸運算及最小化運算來生成。

〔證明〕由例題 2.8, 2.10, 2.9 可知函數 $A(x,y), B(x,y), D(x,y)$ 都是原始遞歸的，因此遞歸函數顯然滿足右列的生成條件。反之，函數 $N(x) = 0$ 是遞歸的（見例題 2.1），又由定理 2.5 證得原始遞歸運算對遞歸函數滿足封閉性，因此右列條件生成的函數必是遞歸的。 ⊠

由以上的定理及例題可知，若一個遞歸函數生成的過程不須經過最小化運算，則它必是一個原始遞歸函數。利用這個關係，我們很容易可判斷函數及敘述是否是原始遞歸的。

定理 **2.8** 若函數 $f(y, x^{(n)})$ 是（原始）遞歸的，則函數

$$h_1(z, x^{(n)}) = \sum_{y=0}^{z} f(y, x^{(n)})$$

與

$$h_2(z, x^{(n)}) = \prod_{y=0}^{z} f(y, x^{(n)})$$

也是（原始）遞歸的。

〔證明〕因為函數 $f(y, x^{(n)})$ 是（原始）遞歸的，所以函數

$$f(0, x^{(n)})$$

也是（原始）遞歸的。令函數

$$\begin{aligned} g_1(z,k,x^{(n)}) &= k + f(z+1,x^{(n)}) \\ &= A\left(U_2^{n+2}(z,k,x^{(n)}), f(S(U_1^{n+2}(z,k,x^{(n)})),x^{(n)})\right), \\ g_2(z,k,x^{(n)}) &= k \cdot f(z+1,x^{(n)}) \\ &= D\left(U_2^{n+2}(z,k,x^{(n)}), f(S(U_1^{n+2}(z,k,x^{(n)})),x^{(n)})\right). \end{aligned}$$

由表示法可看出函數 g_1, g_2 是（原始）遞歸的。又因為函數

$$h_1(z,x^{(n)}), h_2(z,x^{(n)})$$

滿足以下的原始遞歸運算：

$$\begin{aligned} h_1(0,x^{(n)}) &= f(0,x^{(n)}), \\ h_1(z+1,x^{(n)}) &= h_1(z,x^{(n)}) + f(z+1,x^{(n)}) \\ &= g_1(z,h_1(z,x^{(n)}),x^{(n)}), \\ h_2(0,x^{(n)}) &= f(0,x^{(n)}), \\ h_2(z+1,x^{(n)}) &= h_2(z,x^{(n)}) \cdot f(z+1,x^{(n)}) \\ &= g_2(z,h_2(z,x^{(n)}),x^{(n)}). \end{aligned}$$

所以函數 h_1, h_2 是（原始）遞歸的。 ⊠

2.3 原始遞歸集與敘述

定義 **2.4** 設 S 是 N^n 的一個子集合。若特徵函數

$$C_S(x^{(n)}) = \begin{cases} 1, & x^{(n)} \notin S, \\ 0, & x^{(n)} \in S, \end{cases}$$

是一個（原始）遞歸函數，則稱集合 S 是一個（原始）遞歸集。

設 R 是 N^n 的子集合，符號 $\overline{R}$ 代表 R 對 $N^{(n)}$ 的餘集。

定理 **2.9** 若 R, S 是 N^n 的子集合且都是（原始）遞歸集，則集合

$$\overline{R}, R \bigcup S, R \bigcap S$$

也是（原始）遞歸集。

〔證明〕因為原始遞歸集 R, S 的特徵函數 C_R, C_S 是（原始）遞歸的，所以集合 $\overline{R}, R \bigcup S, R \bigcap S$ 的特徵函數

$$\begin{aligned} C_{\overline{R}} &= 1 \dot{-} C_R, \\ C_{R \bigcup S} &= C_R \cdot C_S, \\ C_{R \bigcap S} &= (C_R + C_S) \dot{-} (C_R \cdot C_S), \end{aligned}$$

也是（原始）遞歸的，因此集合 $\overline{R}, R \bigcup S, R \bigcap S$ 是（原始）遞歸集。 ⊠

設 $P(x_1,\cdots,x_n)$ 代表一個關於序對 $x_1,\cdots,x_n$ 的敘述，它的特徵函數 $C_P(x_1,\cdots,x_n)$ 定義如下：

$$C_P(x_1,\ldots,x_n)=\begin{cases}0, & \text{若序對 } x^{(n)} \text{ 滿足敘述 } P(x_1,\cdots,x_n)\\ 1, & \text{其他}\end{cases},$$

若特徵函數 $C_P(x_1,\cdots,x_n)$ 是（原始）遞歸的，則稱敘述 $P(x_1,\cdots,x_n)$ 是（原始）遞歸的。

設 $P(x_1,\cdots,x_n),Q(x_1,\cdots,x_n)$ 是關於 $x^{(n)}$ 的敘述，令

$$\sim P(x_1,\cdots,x_n)$$

代表 P 的否定敘述；

$$P(x_1,\ldots,x_n)\bigvee Q(x_1,\ldots,x_n)$$

代表滿足 P 或 Q 的敘述；

$$P(x_1,\ldots,x_n)\bigwedge Q(x_1,\ldots,x_n)$$

代表同時滿足 P 與 Q 的敘述。

定理 **2.10** 若敘述 $P(x_1,\ldots,x_n),Q(x_1,\ldots,x_n)$ 是（原始）遞歸的，則

$$\sim P(x_1,\ldots,x_n),$$
$$P(x_1,\ldots,x_n)\bigvee Q(x_1,\ldots,x_n),$$
$$P(x_1,\ldots,x_n)\bigwedge Q(x_1,\ldots,x_n)$$

也是（原始）遞歸的。

〔證明〕其證明與定理 2.9 類似，故省略不證。 ☒

定理 2.10 可推廣到不同維度的敘述 $P(x_1,\cdots,x_n),Q(x_1,\cdots,x_m)$，其證明與定理 2.9 類似。

定理 **2.11** 設敘述 $P(y,x^{(n)})$ 是（原始）遞歸的，則敘述

$$\bigvee_{y=0}^{z}P(y,x^{(n)}),\bigwedge_{y=0}^{z}P(y,x^{(n)})$$

也是（原始）遞歸的。

〔證明〕敘述 $\bigvee_{y=0}^{z}P(y,x^{(n)})$ 的特徵函數

$$\prod_{y=0}^{z}C_p(y,x^{(n)})$$

是（原始）遞歸的，所以敘述 $\bigvee_{y=0}^{z}P(y,x^{(n)})$ 是（原始）遞歸的。已知敘述 $\sim P$ 是（原始）遞歸的，因為

$$\bigwedge_{y=0}^{z}P(y,x^{(n)})\leftrightarrow\sim\left[\bigvee_{y=0}^{z}\sim P(y,x^{(n)})\right]$$

所以敘述 $\bigwedge_{y=0}^{z}P(y,x^{(n)})$ 是（原始）遞歸的。 ☒

定義 **2.5** 設 $P(y,x^{(n)})$ 是一個敘述，定義一個變數為 $z,x^{(n)}$ 的函數如下：

$$\mathcal{M}_{y=0}^{z}P(y,x^{(n)})=\begin{cases}\min_y[0\le y\le z\bigwedge P(y,x^{(n)})], & \text{若 } y \text{ 存在},\\ 0, & \text{若 } y \text{ 不存在}.\end{cases},$$

定理 **2.12** 設敘述 $P(y,x^{(n)})$ 是（原始）遞歸的，則函數

$$\mathcal{M}_{y=0}^{z}P(y,x^{(n)})$$

也是（原始）遞歸的。

〔證明〕令函數

$$\rho(t,x^{(n)})=\prod_{y=0}^{t}C_P(y,x^{(n)}),$$

則函數 $\rho(t,x^{(n)})$ 是敘述 $\bigvee_{y=0}^{t}P(y,x^{(n)})$ 的特徵函數。

對序對 $x^{(n)}$ 而言，若非負整數 $t_0(0\le t_0\le z)$ 是使敘述 $P(t_0,x^{(n)})$ 成立的最小值，則

$$\rho(y,x^{(n)})=0,\forall y\ge t_0,$$
$$\rho(y,x^{(n)})=1,\forall y<t_0,$$

我們可推得

$$\begin{aligned}\sum_{t=0}^{z}\rho(t,x^{(n)}) &= \sum_{t=0}^{t_0-1}\rho(t,x^{(n)})+\sum_{t=t_0}^{z}\rho(t,x^{(n)})\\ &= \sum_{t=0}^{t_0-1}1+\sum_{t=t_0}^{z}0\\ &= t_0\\ &= \mathcal{M}_{y=0}^{z}P(y,x^{(n)})\end{aligned}$$

且

$$\alpha(\rho(z,x^{(n)}))=1.$$

若不存在 $t(0\le t\le z)$ 使敘述 $P(t,x^{(n)})$ 成立，則

$$\rho(z,x^{(n)})=1,$$

$$\alpha(\rho(z,x^{(n)}))=0=\mathcal{M}_{y=0}^{z}P(y,x^{(n)}).$$

綜合以上討論，我們可將函數 $\mathcal{M}_{y=0}^{z}P(y,x^{(n)})$ 表示如下：

$$\mathcal{M}_{y=0}^{z}P(y,x^{(n)})=\alpha(\prod_{y=0}^{z}C_P(y,x^{(n)}))\cdot\sum_{t=0}^{z}\prod_{y=0}^{t}C_P(y,x^{(n)}).$$

所以函數 $\mathcal{M}_{y=0}^{z}P(y,x^{(n)})$ 是（原始）遞歸的。 ⊠

下面的敘述及函數皆是（原始）遞歸的：

例題 **2.13** 敘述

$$P(x,y) \leftrightarrow x = y$$

的特徵函數

$$\alpha(\alpha(|x-y|))$$

是（原始）遞歸的，所以敘述“ $x = y$ ”是（原始）遞歸的。

例題 **2.14** 敘述

$$P(x,y) \leftrightarrow y|x$$

可表示為

$$y|x \leftrightarrow \bigvee_{z=0}^{x}(x = yz).$$

因為敘述“ $x = yz$ ”是（原始）遞歸的（特徵函數為 $\alpha(\alpha(|x-yz|))$），所以敘述“ $y|x$ ”是（原始）遞歸的。

例題 **2.15** 敘述

$$P(x,y) \leftrightarrow x < y$$

的特徵函數

$$\alpha(y \dot{-} x)$$

是（原始）遞歸的，所以敘述“ $x < y$ ”是（原始）遞歸的。

例題 **2.16** 敘述

$$P(x,y) \leftrightarrow x \neq y$$

的特徵函數

$$\alpha(|x-y|)$$

是（原始）遞歸的，所以敘述“ $x \neq y$ ”是（原始）遞歸的。

例題 **2.17** 敘述

$$\mathrm{Prime}(x) \leftrightarrow x\text{是一個質數}$$

可表示為

$$\mathrm{Prime}(x) \leftrightarrow (x \neq 1)\bigwedge\bigwedge_{z=0}^{x}\left[(z=1)\bigvee(z=x)\bigvee\sim(z|x)\right].$$

設 0 是一個質數，已知敘述 $x \neq 1, z = 1, z = x,\ z|x$ 皆是（原始）遞歸的，由定理 2.11 可知敘述“ $\mathrm{Prime}(x)$ ”是（原始）遞歸的。

例題 **2.18** 函數 $\mathrm{Pr}(n)$ 代表第 n 個質數的值，設 $\mathrm{Pr}(0) = 0$，因為

$$\begin{aligned} \mathrm{Pr}(0) &= 0, \\ \mathrm{Pr}(n+1) &= \mathcal{M}_{y=0}^{\mathrm{Pr}(n)!+1}[\mathrm{Prime}(y)\bigwedge y > \mathrm{Pr}(n)], \end{aligned}$$

所以函數 $\mathrm{Pr}(n)$ 是（原始）遞歸的。

例題 **2.19** 函數 $[x/2], J(x,y), K(z), L(z)$ 的表示法為：

$$[x/2] = \mathcal{M}^x_{y=0}(2y+2 > x),$$

$$J(x,y) = [((x+y)^2 + 3x + y)/2],$$

$$K(z) = \mathcal{M}^z_{x=0} \bigvee_{y=0}^{z} [z = J(x,y)],$$

$$L(z) = \mathcal{M}^z_{y=0} \bigvee_{x=0}^{z} [z = J(x,y)],$$

所以它們都是（原始）遞歸的。

2.4 圖靈機的計算原理

在第一章中，圖靈機所使用的符號為：

$$R, L, S_0, S_1, \cdots, q_1, q_2, \cdots.$$

令由以上符號所構成的有限排列稱為 表現式。例如：

$$q_1 1111, q_1 1 R q_2, S_2 g_1 B B 1 S_3 R g_2$$

都是表現式。我們將每一個符號對應一個正奇數，其對應如下：

$$\begin{array}{ll} R \to 3, & L \to 5, \\ S_0 \to 7, & q_1 \to 9, \\ S_1 \to 11, & q_2 \to 13, \\ S_2 \to 15, & q_3 \to 17, \\ S_3 \to 19, & q_4 \to 21, \\ \vdots & \vdots \end{array}$$

即對任意 i，符號 S_i 對應 $4i+7$，符號 q_i 對應 $4i+5$。因此表現式 $q_1 1111$ 對應的有限數列為 $9, 11, 11, 11, 11$，$q_1 1 R q_2$ 對應的數列為 $9, 11, 3, 13$，$S_2 g_1 B B 1 S_3 R g_2$ 對應的排列為 $15, 9, 7, 7, 11, 19, 3, 13$。

定義 **2.6** 若表現式 M 由符號 $r_1, r_2, \cdots, r_k$ 依序排列而成，而 $a_1, a_2, \cdots, a_k$ 是其個別對應的數，則我們以 $\mathrm{gn}(M)$ 來代表表現式 M 對應的數，其值定為

$$\mathrm{gn}(M) = \prod_{t=1}^{k} \mathrm{Pr}(t)^{a_t}.$$

若 $M_1, M_2, \cdots, M_l$ 是 l 個表現式依序所成的排列，則我們以 $\mathrm{Gn}(M_1, \cdots, M_l)$ 來表示此排列對應的數，其值定為

$$\mathrm{Gn}(M_1, \cdots, M_l) = \prod_{t=1}^{l} \mathrm{Pr}(t)^{\mathrm{gn}(M_t)}.$$

例如：

$$\begin{aligned}
\mathrm{gn}(q_1 1BS_2) &= 2^9\cdot 3^{11}\cdot 5^7\cdot 7^{15},\\
\mathrm{gn}(q_1 1Rq_2) &= 2^9\cdot 3^{11}\cdot 5^3\cdot 7^{13},\\
\mathrm{Gn}(q_1 1BS_2, q_1 1Rq_2) &= 2^{2^9\cdot 3^{11}\cdot 5^7\cdot 7^{15}}\cdot 3^{2^9\cdot 3^{11}\cdot 5^3\cdot 7^{13}},\\
\mathrm{gn}(q_1 1BS_2 q_1 1Rq_2) &= 2^9\cdot 3^{11}\cdot 5^7\cdot 7^{15}\cdot 11^9\cdot 13^{11}\cdot 17^3\cdot 19^{13}.
\end{aligned}$$

設 $Z=\{M_1,\cdots,M_l\}$ 是一個圖靈機。若

$$z=\mathrm{Gn}(M_1,\cdots,M_l),$$

則我們稱 z 是圖靈機 Z 對應的數。因為此圖靈機有 l 個四元數列，所以圖靈機 Z 共有 $l!$ 種四元數列所成的排列，因此共有 $l!$ 個對應的數。

定義 **2.7** 敘述 $\mathrm{Tn}(z,x_1,\cdots,x_n,y)$ 代表序對 $(z,x_1,\cdots,x_n,y)$ 滿足：z 是某個圖靈機 Z 所對應的數，y 是表示式 $q_1\overline{x_1,\cdots,x_n}$ 對 Z 的算式所對應的數。

例如：設圖靈機 $Z=\{M_1,\cdots,M_l\}$，表示式 $q_1\overline{x_1,\cdots,x_n}$ 對圖靈機 Z 的算式為：

$$\alpha_1\to\cdots\to\alpha_p=\mathrm{Res}_Z(\alpha_1).$$

若

$$\begin{aligned}
z&=\mathrm{Gn}(M_1,\cdots,M_l),\\
y&=\mathrm{Gn}(\alpha_1,\cdots,\alpha_p).
\end{aligned}$$

則 $(z,x_1,\cdots,x_n,y)$ 滿足敘述 $\mathrm{Tn}(z,x_1,\cdots,x_n,y)$。

由下列各敘述及函數的表示法可看出他們都是（原始）遞歸的，利用這些敘述及函數，我們可證明敘述 $\mathrm{Tn}(z,x_1,\cdots,x_n,y)$ 是（原始）遞歸的。

(1) 變數為 n,x 的函數

$$n\mathrm{Gl}x=\mathcal{M}^x_{y=0}[(\mathrm{Pr}(n)^y|x)\bigwedge\sim(\mathrm{Pr}(n)^{y+1}|x)]$$

是（原始）遞歸的。

若 $x=\mathrm{gn}(M)$，M 是由符號 $r_1,\cdots,r_k$ 所組成的表現式，則

$$n\mathrm{Gl}x=\begin{cases} r_n\text{所對應的數}, & 1\le n\le k,\\ 0, & n=0,n>k.\end{cases},$$

若 $\mathrm{Gn}(M_1,\cdots,M_l)$，其中 $M_1,\cdots,M_l$ 是表現式，則

$$n\mathrm{Gl}x=\begin{cases}\mathrm{gn}(M_n), & 0<n\le l,\\ 0, & n=0,n>l.\end{cases}$$

(2) 函數

$$\mathcal{L}(x)=\mathcal{M}^x_{y=0}[(y\mathrm{Gl}x>0)\bigwedge\bigwedge\nolimits^x_{i=0}(y+i+1)\mathrm{Gl}x=0]$$

是（原始）遞歸的。若 $x=\mathrm{gn}(M)$，M 是由符號 $r_1,\cdots,r_k$，所組成的表現式，則 $\mathcal{L}(x)=k$。若 $x=\mathrm{Gn}(M_1,\cdots,M_l)$，其中 $M_1,\cdots,M_l$ 是表現式，則 $\mathcal{L}(x)=l$。

(3) 敘述

$$\mathrm{GN}(x) \leftrightarrow\sim \bigvee_{y=0}^{\mathcal{L}(x)} [((y\mathrm{Gl}x = 0) \bigwedge (y+1)\mathrm{Gl}x \neq 0)]$$

是（原始）遞歸的。敘述 $\mathrm{GN}(x)$ 成立的充分必要條件是存在正整數 $a_k, 1 \leq k \leq n$，使得

$$x = \prod_{k=1}^{n} \mathrm{Pr}(k)^{a_k}.$$

(4) 敘述

$$\mathrm{Term}(x,z) \leftrightarrow \mathrm{GN}(z) \bigwedge \bigvee_{n=0}^{\mathcal{L}(x)} [(x = n\mathrm{Gl}z) \bigwedge (n \neq 0)]$$

是（原始）遞歸的。敘述 $\mathrm{Term}(x,z)$ 成立的充分必要條件是存在一個適當的 $a_k > 0$ 使得

$$z = \prod_{k=1}^{n} \mathrm{Pr}(k)^{a_k}$$

且 x 為其中一個 $a_k, 1 \leq k \leq n$。

(5) 函數

$$x * y = x \cdot \prod_{i=0}^{\mathcal{L}(y)\dot{-}1} \mathrm{Pr}(L(x)+i+1)^{(i+1)\mathrm{Gl}y}$$

是（原始）遞歸的。若 M, N 皆為表現式，則 $\mathrm{gn}(MN) = \mathrm{gn}(M) * \mathrm{gn}(N)$。若

$$x = \mathrm{Gn}(M_1, \cdots, M_n), y = \mathrm{Gn}(N_1, \cdots, N_k),$$

則

$$x * y = \mathrm{Gn}(M_1, \cdots, M_n, N_1, \cdots, N_k).$$

(6) 敘述

$$\mathrm{IC}(x) \leftrightarrow \bigvee_{y=0}^{x} (x = 4y + 9)$$

是（原始）遞歸的。敘述 $\mathrm{IC}(x)$ 成立的充分必要條件為 x 是某一個 q_i 對應的數。

(7) 敘述

$$\mathrm{Al}(x) \leftrightarrow \bigvee_{y=0}^{x} (x = 4y + 7)$$

是（原始）遞歸的。敘述 $\mathrm{Al}(x)$ 成立的充分必要條件為 x 是某一個 S_i 對應的數。

(8) 敘述

$$\mathrm{Odd}(x) \leftrightarrow \bigvee_{y=0}^{x}(x = 2y + 3)$$

是（原始）遞歸的。

敘述 $\mathrm{Odd}(x)$ 成立的充分必要條件為 x 是某一個大於等於 3 的奇數。

(9) 敘述

$$\mathrm{Quad}(x) \leftrightarrow \mathrm{GN}(x) \bigwedge (\mathcal{L}(x) = 4)$$

$$\bigwedge \mathrm{IC}(1\mathrm{Gl}x) \bigwedge \mathrm{Al}(2\mathrm{Gl}x) \bigwedge \mathrm{Odd}(3\mathrm{Gl}x) \bigwedge \sim \mathrm{IC}(3\mathrm{Gl}x) \bigwedge \mathrm{IC}(4\mathrm{Gl}x)$$

是（原始）遞歸的。敘述 $\mathrm{Quad}(x)$ 成立的充分必要條件為 x 是某一個四元數列對應的數。

(10) 敘述

$\mathrm{Inc}(x, y) \leftrightarrow \mathrm{Quad}(x) \bigwedge \mathrm{Quad}(y)$
$\bigwedge (1\mathrm{Gl}x = 1\mathrm{Gl}y) \bigwedge (2\mathrm{Gl}x = 2\mathrm{Gl}y) \bigwedge (x \neq y)$
是（原始）遞歸的。敘述 $\mathrm{Inc}(x, y)$ 成立的充分必要條件為 x, y 分別代表兩個四元數列所對應的數，且這兩個四元數列的前兩個符號相同。

(11) 敘述

$$\mathrm{TM}(x) \leftrightarrow \mathrm{GN}(x) \bigwedge \bigwedge_{n=1}^{\mathcal{L}(x)} \left[\mathrm{Quad}(n\mathrm{Gl}x) \bigwedge \bigwedge_{m=1}^{\mathcal{L}(x)} \sim (\mathrm{Inc}(n\mathrm{Gl}x, m\mathrm{Gl}x)) \right]$$

是（原始）遞歸的。敘述 $\mathrm{TM}(x)$ 成立的充分必要條件為 x 是某個圖靈機對應的數。

(12) 函數

$$\mathrm{MR}(n) = \mathrm{gn}(1^{n+1}) = \mathrm{gn}(\overline{n})$$

是（原始）遞歸的。因為

$$\begin{aligned} \mathrm{MR}(0) &= 2^{11}, \\ \mathrm{MR}(n+1) &= 2^{11} * \mathrm{MR}(n). \end{aligned}$$

(13) 函數 $\mathrm{CU}(n, x)$ 滿足：

$$\mathrm{CU}(n, x) = \begin{cases} 0, & 若 n\mathrm{GL}x \neq 11, \\ 1, & 若 n\mathrm{GL}x = 11. \end{cases}$$

是（原始）遞歸的。因為函數 $\mathrm{CU}(n, x)$ 是（原始）遞歸敘述 $n\mathrm{GL}x \neq 11$ 的特徵函數。

(14) 函數

$$\mathrm{Corn}(x) = \sum_{n=1}^{\mathcal{L}(x)} \mathrm{CU}(n, x)$$

是（原始）遞歸的。若 $x = \mathrm{gn}(M)$，則 $\mathrm{Corn}(x) = \langle M \rangle$。

(15) 函數

$$U(y) = \mathrm{Corn}(\mathcal{L}(y)Gly)$$

是（原始）遞歸的。若 $y = \mathrm{Gn}(M_1, \cdots, M_n)$，則 $U(y) = \langle M_n \rangle$。

(16) 敘述

$$\mathrm{ID}(x) \leftrightarrow \mathrm{GN}(x) \bigwedge \bigvee_{n=1}^{\mathcal{L}(x) \dot{-} 1} \{IC(nGlx) \bigwedge \bigwedge_{m=1}^{\mathcal{L}(x)} [(m = n) \bigvee \mathrm{Al}(mGlx)]\}$$

是（原始）遞歸的。敘述 $\mathrm{ID}(x)$ 成立的充分必要條件是 x 是一個表現式對應的數。

(17) 函數

$$\mathrm{Init}_n(x_1, \cdots, x_n) = 2^9 * \mathrm{MR}(x_1) * 2^7 * \mathrm{MR}(x_2) * 2^7 * \cdots * \mathrm{MR}(x_n)$$

是（原始）遞歸的。即 $\mathrm{Init}_n(x_1, \cdots, x_n) = \mathrm{gn}(q_1(x_1, \cdots, x_n))$。

(18) 敘述

$$\mathrm{Yield}_1(x, y, z) \leftrightarrow \mathrm{ID}(x) \bigwedge \mathrm{ID}(y) \bigwedge \mathrm{TM}(z)$$

$$\bigwedge \{ \bigvee_{F=0}^{x} \bigvee_{G=0}^{x} \bigvee_{r=0}^{x} \bigvee_{s=0}^{x} \bigvee_{t=0}^{x} \bigvee_{u=0}^{x} [(x = F * 2^r * 2^s * G)]$$

$$\bigwedge (y = F * 2^t * 2^u * G) \bigwedge \mathrm{IC}(r) \bigwedge \mathrm{IC}(t) \bigwedge \mathrm{Al}(s) \bigwedge \mathrm{Al}(u)$$

$$\bigwedge \mathrm{Term}(2^r * 3^s * 5^u * 7^t, z)]\}$$

是（原始）遞歸的。敘述 $\mathrm{Yield}(x, y, z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，x, y 分別代表某兩個表示式 M_1, M_2 對應的數，且

$$M_1 \to M_2(Z)$$

滿足定義 1.2 的第一個情況。

(19) 敘述

$$\mathrm{Yield}_2(x, y, z) \leftrightarrow \mathrm{ID}(x) \bigwedge \mathrm{ID}(y) \bigwedge \mathrm{TM}(z)$$

$$\bigwedge \{ \bigvee_{F=0}^{x} \bigvee_{G=0}^{x} \bigvee_{r=0}^{x} \bigvee_{s=0}^{x} \bigvee_{t=0}^{x} \bigvee_{u=0}^{x} [(x = F * 2^r * 2^s * 2^t * G)]$$

$$\bigwedge (y = F * 2^s * 2^u * 2^t * G) \bigwedge \mathrm{IC}(r) \bigwedge \mathrm{IC}(u) \bigwedge \mathrm{Al}(s) \bigwedge \mathrm{Al}(t)$$
$$\bigwedge \mathrm{Term}(2^r * 3^s * 5^3 * 7^u, z)]\}$$

是（原始）遞歸的。敘述 $\mathrm{Yield}(x, y, z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，x, y 分別代表某兩個表示式 M_1, M_2 對應的數，且

$$M_1 \to M_2(Z)$$

滿足定義 1.2 的第二個情況。

(20) 敘述

$\mathrm{Yield}_3(x,y,z) \leftrightarrow \mathrm{ID}(x) \bigwedge \mathrm{ID}(y) \bigwedge \mathrm{TM}(z)$

$\bigwedge\{\bigvee_{F=0}^{x}\bigvee_{G=0}^{x}\bigvee_{r=0}^{x}\bigvee_{s=0}^{x}\bigvee_{t=0}^{x}\bigvee_{u=0}^{x}[(x = F * 2^r * 2^s)]$

$\bigwedge(y = F * 2^s * 2^t * 2^7) \bigwedge \mathrm{IC}(r) \bigwedge \mathrm{IC}(t) \bigwedge \mathrm{Al}(s)$

$\bigwedge \mathrm{Term}(2^s * 3^t * 5^3 * 7^u, z)]\}$

是（原始）遞歸的。敘述 $\mathrm{Yield}(x,y,z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，x,y 分別代表某兩個表示式 M_1, M_2 對應的數，且

$$M_1 \to M_2(Z)$$

滿足定義 1.2 的第三個情況。

(21) 敘述

$\mathrm{Yield}_4(x,y,z) \leftrightarrow \mathrm{ID}(x) \bigwedge \mathrm{ID}(y) \bigwedge \mathrm{TM}(z)$

$\bigwedge\{\bigvee_{F=0}^{x}\bigvee_{G=0}^{x}\bigvee_{r=0}^{x}\bigvee_{s=0}^{x}\bigvee_{t=0}^{x}\bigvee_{u=0}^{x}[(x = F * 2^r * 2^s * 2^t * G)]$

$\bigwedge(y = F * 2^u * 2^r * 2^t * G) \bigwedge \mathrm{IC}(s) \bigwedge \mathrm{IC}(u) \bigwedge \mathrm{Al}(r) \bigwedge \mathrm{Al}(t)$
$\bigwedge \mathrm{Term}(2^s * 3^t * 5^5 * 7^u, z)]\}$

是（原始）遞歸的。敘述 $\mathrm{Yield}(x,y,z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，x,y 分別代表某兩個表示式 M_1, M_2 對應的數，且

$$M_1 \to M_2(Z)$$

滿足定義 1.2 的第四個情況。

(22) 敘述

$\mathrm{Yield}_5(x,y,z) \leftrightarrow \mathrm{ID}(x) \bigwedge \mathrm{ID}(y) \bigwedge \mathrm{TM}(z)$

$\bigwedge\{\bigvee_{G=0}^{x}\bigvee_{r=0}^{x}\bigvee_{s=0}^{x}\bigvee_{t=0}^{x}\bigvee_{u=0}^{x}[(x = 2^r * 2^s * G)]$

$\bigwedge(y = 2^t * 2^7 * 2^s * G) \bigwedge \mathrm{IC}(s) \bigwedge \mathrm{IC}(t) \bigwedge \mathrm{Al}(s)$

$\bigwedge Term(2^r * 3^s * 5^5 * 7^t, z)]\}$

是（原始）遞歸的。敘述 $\mathrm{Yield}_5(x,y,z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，x,y 是分別代表某兩個表示式 M_1, M_2 對應的數，且

$$M_1 \to M_2(Z)$$

滿足定義 1.2 的第五個情況。

(23) 敘述

$\mathrm{Yield}(x,y,z) \leftrightarrow \mathrm{Yield}_1(x,y,z) \bigvee \mathrm{Yield}_2(x,y,z)$

$\bigvee \mathrm{Yield}_3(x,y,z) \bigvee \mathrm{Yield}_4(x,y,z) \bigvee \mathrm{Yield}_5(x,y,z)$

是（原始）遞歸的。敘述 $\mathrm{Yield}(x,y,z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，x,y 分別代表某兩個表示式 M_1,M_2 對應的數，且

$$M_1 \to M_2(Z)$$

滿足定義 1.2 的任何一種情況。

(24) 敘述

$$\mathrm{Fin}(x,z) \leftrightarrow \mathrm{ID}(x) \bigwedge \mathrm{TM}(z)$$
$$\bigwedge \bigvee_{F=0}^{x} \bigvee_{F=0}^{x} \bigvee_{s=0}^{x} \{(x = F * 2^r * 2^s * G) \bigwedge \mathrm{IC}(r) \bigwedge \mathrm{Al}(s)$$
$$\bigwedge \bigwedge_{n=1}^{\mathcal{L}(z)} [(1\mathrm{Gl}(n\mathrm{Gl}z) \neq r) \bigvee (2\mathrm{Gl}(n\mathrm{Gl}z) \neq s)]\}$$

是（原始）遞歸的。敘述 $\mathrm{Fin}(x,z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，x 圖靈機 Z 的一個終結式所對應的數。

(25) 敘述

$$\mathrm{Comp}(y,z) \leftrightarrow \mathrm{TM}(z) \bigwedge \mathrm{GN}(y) \bigwedge \bigwedge_{n=1}^{\mathcal{L}(y)\dot{-}1} \mathrm{Yield}(n\mathrm{Gl}y, (n+1)\mathrm{Gl}y, z)$$
$$\bigwedge \mathrm{Fin}(\mathcal{L}(y)\mathrm{Gl}y, z)$$

是（原始）遞歸的。敘述 $\mathrm{Comp}(y,z)$ 成立的充分必要條件為：z 是某個圖靈機 Z 對應的數，y 是此圖靈機 Z 的算式所對應的數。

2.5 可計算函數是遞歸的

定理 **2.13** 敘述 $\mathrm{Tn}(z,x_1,\cdots,x_n,y)$ 是（原始）遞歸的。

〔證明〕敘述 $\mathrm{Tn}(z,x_1,\cdots,x_n,y)$ 可表示為

$$\mathrm{Tn}(z,x_1,\cdots,x_n,y) \leftrightarrow \mathrm{Comp}(y,z) \bigwedge (1\mathrm{Gl}y = \mathrm{Init}_n(x_1,\cdots,x_n)).$$

由表示法可知敘述 $\mathrm{Tn}(z,x_1,\cdots,x_n,y)$ 是（原始）遞歸的。 ☒

定理 **2.14** 可計算函數都是遞歸的。

〔證明〕若函數 $f(x^{(n)})$ 是一個可計算函數，則存在一個圖靈機 Z_0，使得

$$f(x^{(n)}) = \psi_{Z_0}^{(n)}(x^{(n)}).$$

設 z_0 是圖靈機 Z_0 對應的數，因為敘述 $\mathrm{Tn}(z,x^{(n)},y)$ 是原始遞歸的，所以其特徵函數

$$C_{\mathrm{Tn}}(z,x^{(n)},y) = \begin{cases} 0, & (z,x^{(n)},y) \in \mathrm{Tn}(z,x^{(n)},y), \\ 1, & \text{其他}. \end{cases}$$

是一個原始遞歸函數。設表示式 $\alpha_1 = q_1\overline{x^{(n)}}$ 對圖靈機 Z_0 的算式為：

$$\alpha_1 \to \alpha_2 \to \cdots \to \alpha_p = \mathrm{Res}_{Z_0}(\alpha_1)$$

則

$$\begin{aligned} f(x^{(n)}) &= \psi^{(n)}_{Z_0}(x^{(n)}) \\ &= \langle \alpha_p \rangle \\ &= U(\mathrm{Gn}(\alpha_1, \cdots, \alpha_p)) \\ &= U\left(\min_y [C_{Tn}(z_0, x^{(n)}, y) = 0]\right). \end{aligned}$$

由表示法我們可得出可計算函數是遞歸的。 ⊠

由以上的結果，我們得到本章的結論：

定理 **2.15** 一個函數是可計算的其充份必要條件為它是遞歸的。

第 3 章

刁藩圖集（Diophantine Set）

本章的目的是在證出一般所熟悉的算術函數，如

$$a = \alpha_b(c), b^c, \binom{n}{m}, m!$$

都是刁藩圖函數，並證明通用刁藩圖函數的存在。利用此通用刁藩圖方程式得出一個 1 維的刁藩圖集 S，其餘集 $N - S$ 卻不是刁藩圖集。

3.1 刁藩圖集

刁藩圖方程式 (Diophantine equation) 是指以整數為係數的多項式方程式。例如：

$$xy + 2x + 2y - a = 0, x^5y^3 + y^2z^3 - 2z^6 = 0, \cdots$$

等都是刁藩圖方程式。我們習慣將變數為 $a_1, \cdots, a_n, x_1, \cdots, x_m$ 的刁藩圖方程式

$$D(a_1, \cdots, a_n, x_1, \cdots, x_m) = 0$$

區分為參數 $a_1, \cdots, a_n$ 與未知數 $x_1, \cdots, x_m$。

定義 **3.1** 設 S 是集合 N^n 的一個子集合。如果存在一個刁藩圖方程式

$$D(a_1, \cdots, a_n, x_1, \cdots, x_m) = 0,$$

使得 $(a_1, \cdots, a_n) \in S$ 的充份必要條件為存在 $(x_1, \cdots, x_m) \in N^m$ 使得

$$D(a_1, \cdots, a_n, x_1, \cdots, x_m) = 0,$$

則稱 S 是一個 n 維度的 刁藩圖集(Diophantine set)，或稱集合 S 是刁藩圖的。我們習慣把刁藩圖集 S 用邏輯式子

$$(a_1, a_2, \cdots, a_n) \in S \Longleftrightarrow \exists x_1, \cdots, x_m[D(a_1, \cdots, a_n, x_1, \cdots, x_m) = 0]$$

來描述，並稱此方程式

$$D(a_1, \cdots, a_n, x_1, \cdots, x_m) = 0$$

為集合 S 的一個刁藩圖表現(Diophantine representation)。

例題 **3.1** 以下的集合都是 1 維度的刁藩圖集。

(1) 所有非負偶數所構成的集合 $A = \{0, 2, 4, 6, 8, \cdots\}$ 是刁藩圖的。這是因為

$$a \in A \Longleftrightarrow \exists x \, [\, a - 2x = 0].$$

(2) 所有非負奇數所構成的集合 $B = \{1, 3, 5, 7, 9, \cdots\}$ 是刁藩圖的。這是因為

$$a \in B \Longleftrightarrow \exists x \, [\, a - (2x + 1) = 0].$$

(3) 所有正的合成數所構成的集合 C 是刁藩圖的。這是因為

$$a \in C \Longleftrightarrow \exists x_1, x_2 \, [\, a - (x_1 + 2)(x_2 + 2) = 0].$$

(4) 所有不是 2 的次方冪的非負整數所構成的集合 $D = N - \{2^0, 2^1, 2^2, 2^3, \cdots\}$ 是刁藩圖的。這是因為

$$a \in D \Longleftrightarrow \exists x_1, x_2 \, [\, a - x_1(2x_2 + 3) = 0].$$

(5) 所有質數所構成的集合 $\{2, 3, 5, 7, \cdots\}$ 也是刁藩圖的，我們留在以後證明這個相當重要的結果。

例題 **3.2** 以下的集合都是 2 維度的刁藩圖集。

(1) 集合 $E = \{(a, b) \in N^2 |\, a < b\}$ 是刁藩圖的。這是因為

$$(a, b) \in E \Longleftrightarrow \exists x \, [\, a + 1 - b + x = 0].$$

(2) 集合 $F = \{(a, b) \in N^2 | a \leq b\}$ 是刁藩圖的。這是因為

$$(a, b) \in F \Longleftrightarrow \exists x \, [\, a - b + x = 0].$$

(3) 集合 $G = \{(a, b) \in N^2 |\, a \neq b\}$ 是刁藩圖的。這是因為

$$(a, b) \in G \Longleftrightarrow \exists x \, [\, (a - b)^2 - (x + 1) = 0].$$

(4) 集合 $H = \{(a, b) \in N^2 |\, a|b\}$ 是刁藩圖的。這是因為

$$(a, b) \in H \Longleftrightarrow \exists x \, [\, ax - b = 0].$$

定理 **3.1** 如果集合 S_1, S_2 是兩個 n 維度的刁藩圖集，則聯集 $S_1 \cup S_2$ 與交集 $S_1 \cap S_2$ 也都是 n 維度的刁藩圖集。

〔證明〕設刁藩圖集 S_1, S_2 的刁藩圖表現分別為：

$$D_1(a_1, \cdots, a_n, x_1, \cdots, x_{m_1}) = 0,$$

與

$$D_2(a_1, \cdots, a_n, x_1, \cdots, x_{m_2}) = 0.$$

很容易可看出新的刁藩圖方程式

$$D_1(a_1,\cdots,a_n,x_1,\cdots,x_{m_1})\cdot D_2(a_1,\cdots,a_n,x_1,\cdots,x_{m_2})=0$$

與

$$D_1^2(a_1,\cdots,a_n,x_1,\cdots,x_{m_1})+D_2^2(a_1,\cdots,a_n,x_1,\cdots,x_{m_2})=0$$

分別是 $S_1\cup S_2$ 與 $S_1\cap S_2$ 的刁藩圖表現。 ⊠

我們可以將一個低維度的刁藩圖集擴充成較高維度的刁藩圖集。程序如下：假設 S 是一個 n 維度的刁藩圖集，且它的邏輯式子為

$$(a_1,\cdots,a_n)\in S\Longleftrightarrow\exists x_1,\cdots,x_k[D(a_1,\cdots,a_n,x_1,\cdots,x_k)=0].$$

設 m 是一個正整數且令集合 S_m 為

$$S_m=\{(a_1,\cdots,a_n,b_1,\cdots,b_m)|(a_1,\cdots,a_n)\in S,b_i\in N,i=1,\cdots,m\}.$$

很容易可檢驗出刁藩圖方程式

$$D(a_1,\cdots,a_n,x_1,\cdots,x_k)=0,$$

亦是 S_m 的刁藩圖表現，所以 S_m 是一個 $n+m$ 維度的刁藩圖集。例如：由例題 3.2(2) 知道，$\{(a,b,c)\in N^3|a<c\}$ 是刁藩圖的。

設 b 為整數，c 為正整數，我們利用符號 $b\operatorname{div}c,\operatorname{rem}(b,c)$ 代表 b 除以 c 的商及餘數；用符號 $\operatorname{arem}(b,c)$ 代表

$$\min\{|x|\mid x\equiv b\pmod c\},$$

並規定函數 $b\operatorname{div}c,\operatorname{rem}(b,c),\operatorname{arem}(b,c)$ 在 $c=0$ 時沒有定義。設 $\gcd(b,c)$ 代表正整數 b,c 的最大公因數，$\operatorname{lcm}(b,c)$ 代表正整數 b,c 的最小公倍數。當 b 與 c 有一不為正整數時，規定函數 $\gcd(b,c)$ 與 $\operatorname{lcm}(b,c)$ 沒有定義。

例題 **3.3** 以下的集合都是刁藩圖集：

(1) 集合 $I=\{(a,b,c)\in N^3|a=\operatorname{rem}(b,c)\}$ 是刁藩圖的。這是因為

$$a=\operatorname{rem}(b,c)\Longleftrightarrow a<c\bigwedge c|(b-a),$$

所以 I 是刁藩圖集 $\{(a,b,c)\in N^3|a<c\}$ 與刁藩圖集

$$\{(a,b,c)\in N^3|c|(b-a)\}$$

的交集。由定理 3.1 知：I 是刁藩圖的。

(2) 集合 $J=\{(a,b,c)\in N^3|a=b\operatorname{div}c\}$ 是刁藩圖的。這是因為

$$a=b\operatorname{div}c\iff 0\le b-ac<c$$

所以 J 是刁藩圖集 $\{(a,b,c)\in N^3|0<b-ac\}$ 與刁藩圖集

$$\{(a,b,c)\in N^3|b-ac<c\}$$

的交集。

(3) 集合 $K = \{(a,b,c) \in N^3 | a \equiv b \pmod{c}\}$ 是刁藩圖的。這是因為

$$a \equiv b \pmod{c} \Longleftrightarrow c > 0 \bigwedge c|(a-b).$$

所以 K 是刁藩圖集 $\{(a,b,c) \in N^3 | c > 0\}$ 與刁藩圖集

$$\{(a,b,c) \in N^3 | c|(a-b)\}$$

的聯集。由定理 3.1 知：K 是刁藩圖的。

(4) 集合 $L = \{(a,b,c) \in N^3 | a = \gcd(b,c)\}$ 是刁藩圖的。這是因為

$$a = \gcd(b,c) \Longleftrightarrow bc > 0 \bigwedge a|b \bigwedge a|c \bigwedge \exists x,y[a = bx - cy],$$

所以 L 是刁藩圖的。集合 $M = \{(a,b,c) \in N^3 | a = \mathrm{lcm}(b,c)\}$ 也是刁藩圖的。這是因為 $bc = \gcd(b,c)\mathrm{lcm}(b,c)$ 及

$$a = \mathrm{lcm}(b,c) \iff \exists x,y,z[bc = ax \bigwedge bc > 0 \bigwedge x|b \bigwedge x|c \bigwedge x = by - cz],$$

所以 M 是刁藩圖的。

(5) 集合 $N = \{(a,b,c) \in N^3 | a = \mathrm{arem}(b,c)\}$ 是刁藩圖的。這是因為

$$a = \mathrm{arem}(b,c) \iff c > 0 \bigwedge 0 \le 2a \le c \bigwedge [\, c|(b-a) \bigvee c|(b+a) \,].$$

3.2 冪函數與指數函數都是刁藩圖函數

設集合 $S \subset N^n$ 且函數 $f : S \to N$。如果函數 $f(x_1, x_2, \cdots, x_n)$ 的<u>圖</u> (graph)

$$\{(x_1, \cdots, x_n, y) \in N^{n+1} \mid (x_1, \cdots, x_n) \in S, y = f(x_1, \cdots, x_n)\}$$

是一個刁藩圖集，則稱 $f(x_1, x_2, \cdots, x_n)$ 是一個 <u>刁藩圖函數</u> (Diophantine function)，或稱函數 f 是刁藩圖的。

例題 **3.4** 下列的函數都是刁藩圖函數。

(1) 因為 $I = \{(a,b,c) \in N^3 |\ a = \mathrm{rem}(b,c)\}$ 是刁藩圖的，所以函數 $\mathrm{rem}(b,c)$ 是刁藩圖的。

(2) 因為 $N = \{(a,b,c) \in N^3 |\ a = \mathrm{arem}(b,c)\}$ 是刁藩圖的，所以函數 $\mathrm{arem}(b,c)$ 是刁藩圖的。

(3) 因為 $J = \{(a,b,c) \in N^3 |\ a = b \operatorname{div} c\}$ 是刁藩圖的，所以函數 $b \operatorname{div} c$ 是刁藩圖的。

(4) 因為 $L = \{(a,b,c) \in N^3 \mid a = \gcd(b,c)\}, M = \{(a,b,c) \in N^3 \mid a = \mathrm{lcm}(b,c)\}$ 是刁藩圖的，所以函數 $\gcd(b,c), \mathrm{lcm}(b,c)$ 是刁藩圖的。

(5) 函數

$$R(x,y) = \left\{ \begin{array}{ll} 0, & y = 0, \\ x \operatorname{div} y, & y \neq 0 \end{array} \right\}.$$

是刁藩圖的。這是因為集合

$$\{(x,y,z) | z = R(x,y)\} = \{(x,y,z) | z = \mathrm{rem}(x,y) \bigvee (y = 0 \bigwedge z = 0)\}$$

是刁藩圖的，所以函數 $R(x,y)$ 是刁藩圖的。

(6) 第二章定理 2.2 中的函數 $J(x,y), K(z), L(z)$ 都是刁藩圖的。這是因為

$$J(K(z), L(z)) = z$$

及

$$z = J(x,y) \Longleftrightarrow 2z = (x+y)^2 + 3x + y,$$
$$x = K(z) \Longleftrightarrow \exists y\ [2z = (x+y)^2 + 3x + y],$$
$$y = L(z) \Longleftrightarrow \exists x\ [2z = (x+y)^2 + 3x + y].$$

為了證明冪函數 x^y 是一個刁藩圖函數，我們需要考慮底下的數列。設 $b \geq 2$ 為一個正整數且數列 $\langle \alpha_b(n) \rangle$ 滿足如下條件：

$$\alpha_b(-1) = -1, \alpha_b(0) = 0,\ \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n), (n \geq -1).$$

設矩陣

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix},$$

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$E_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}.$$

我們有

$$A_b(0) = E, A_b(n+1) = A_b(n)E_b, A_b(n) = E_b^n, \tag{3.1}$$

因此

$$\det A_b(n) = 1,$$

即

$$\alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1) = 1.$$

利用以上的結果，我們可以證明

定理 **3.2** 設 (x,y) 是方程組

$$x^2 - bxy + y^2 = 1, x > y \tag{3.2}$$

的一個非負整數解的充份必要條件為存在一個 $m \in N$ 使得

$$x = \alpha_b(m+1),\ y = \alpha_b(m). \tag{3.3}$$

〔證明〕對任意 $m \in N$,

$$x = \alpha_b(m+1), y = \alpha_b(m)$$

顯然是方程組 (3.2) 的非負整數解。反之，若 (x,y) 是方程組 (3.2) 的所有非負整數解中，不滿足 (3.3) 且 x 值是最小的一組解。令

$$x_1 = y, y_1 = by - x. \tag{3.4}$$

因為 $x^2 - bxy + y^2 = 1, y \geq 1, x > y$，所以

$$\begin{aligned} y_1 &= by - x = \frac{y^2 - 1}{x} \geq 0, \\ x_1 - y_1 &= x + y - by = \frac{x^2 + xy - bxy}{x} = \frac{xy - y^2 + 1}{x} > 0. \end{aligned}$$

又因為

$$\begin{aligned} x_1^2 - bx_1y_1 + y_1^2 &= y^2 - by(by - x) + (by - x)^2 \\ &= x^2 - bxy + y^2 \\ &= 1, \end{aligned}$$

所以 (x_1, y_1) 也是方程組 (3.2) 的一組解，而且 $x_1 = y < x$。由假設知道：存在一個 $m \in N$, 使得

$$x_1 = \alpha_b(m+1), y_1 = \alpha_b(m).$$

代入 (3.4) 得到

$$\begin{aligned} x &= bx_1 - y_1 = \alpha_b(m+2), \\ y &= x_1 = \alpha_b(m+1). \end{aligned}$$

此與原先的假設矛盾。故方程組 (3.2) 的通解為

$$x = \alpha_b(m+1),\ y = \alpha_b(m), \quad m \in N.$$

⊠

定理 **3.3** 若 $\alpha_b^2(k) | \alpha_b(m)$, 則 $\alpha_b(k) | m$.

〔證明〕令 $m = kl + n, 0 \leq n < k$，因為

$$\begin{aligned} &\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ &= A_b(m) \\ &= E_b^m \\ &= E_b^{n+kl} \\ &= E_b^n (E_b^k)^l \\ &= A_b(n) A_b^l(k) \\ &= \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^l, \end{aligned}$$

我們有

$$\begin{aligned} &\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ &\equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^l \pmod{\alpha_b(k)}, \end{aligned}$$

並比較左下角的元素得到

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^l(k+1) \pmod{\alpha_b(k)}.$$

因為 $\alpha_b(k)$ 與 $\alpha_b(k+1)$ 互質，所以 $\alpha_b(k)$ 整除 $\alpha_b(n)$。又因為 $\alpha_b(n) < \alpha_b(k)$，所以 $n = 0$，也就是 $m = kl$。代回原式可得到

$$\begin{aligned} A_b(m) &= A_b^l(k) \\ &= (\alpha_b(k)E_b - \alpha_b(k-1)E)^l \\ &= \sum_{i=0}^{l}(-1)^{l-i}\binom{l}{i}\alpha_b^i(k)\alpha_b^{l-i}(k-1)E_b^i. \end{aligned}$$

因此

$$\begin{aligned} A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ &\equiv (-1)^l\alpha_b^l(k-1)E + (-1)^{l-1}l\alpha_b(k)\alpha_b^{l-1}(k-1)E_b \pmod{\alpha_b^2(k)}, \end{aligned}$$

比較左下角的元素得到

$$\alpha_b(m) \equiv (-1)^{l-1}l\alpha_b(k)\alpha_b^{l-1}(k-1) \pmod{\alpha_b^2(k)}. \tag{3.5}$$

利用 $\alpha_b^2(k)|\alpha_b(m)$，得到

$$\alpha_b(k)|l\alpha_b^{l-1}(k-1).$$

又因為 $\alpha_b(k), \alpha_b(k-1)$ 互質，所以

$$\alpha_b(k)|l,$$

即

$$\alpha_b(k)|m.$$

⊠

定理 **3.4** 設 a, b, c 為非負整數。證明：$b \geq 4, c \geq 0$ 及 $a = \alpha_b(c)$ 的充份必要條件為下列方程組有非負整數解 u, t, s, r, v, w, x 與 y。

$$b \geq 4, \tag{3.6}$$

$$u^2 - but + t^2 = 1, \tag{3.7}$$

$$s^2 - bsr + r^2 = 1, \tag{3.8}$$

$$r < s, \tag{3.9}$$

$$u^2|s, \tag{3.10}$$

$$v = bs - 2r, \tag{3.11}$$

$$v|w - b, \tag{3.12}$$

$$u|w - 2, \tag{3.13}$$

$$w > 2, \tag{3.14}$$

$$x^2 - wxy + y^2 = 1, \tag{3.15}$$

$$2a < u, \tag{3.16}$$

$$a = \mathrm{arem}(x, v), \tag{3.17}$$

$$c = \mathrm{arem}(x, u). \tag{3.18}$$

也就是說，集合 $\{(a,b,c) \in N^3 \mid b \geq 4 \bigwedge a = \alpha_b(c)\}$ 是刁藩圖的，即函數 $\alpha_b(c)$（定義域為 $(b,c) \in \{4,5,\cdots,\} \times N)$）是刁藩圖的。

〔證明〕先證明若 a,b,c 滿足方程組 (3.6) $\sim$ (3.18)，則 $b \geq 4, c \geq 0$ 且 $a = \alpha_b(c)$. 由 (3.6), (3.7), 定理 3.2 及 (3.10) 可知存在一個 $k \in N$ 使得

$$u = \alpha_b(k) > 0; \tag{3.19}$$

同理，由 (3.6), (3.8) 及 (3.9) 可知存在一個正整數 m 使得

$$s = \alpha_b(m),\ r = \alpha_b(m-1). \tag{3.20}$$

由 (3.11), (3.20) 及數列 $\langle \alpha_b(m) \rangle$ 可知

$$v = bs - 2r = \alpha_b(m+1) - \alpha_b(m) > 0. \tag{3.21}$$

由 (3.10), (3.19) 及 (3.20) 及定理 3.3 可得到

$$u | m. \tag{3.22}$$

又由 (3.14) 及 (3.15) 可知存在一個 $n \in N$ 使得

$$x = \alpha_w(n). \tag{3.23}$$

若 $w \equiv b \pmod{v}$，則 $x = \alpha_w(n) \equiv \alpha_b(n) \pmod{v}$（由數學歸納法可證得，在此省略不證）。因為 $\alpha_2(n) = n$，所以由 (3.12) 及 (3.13) 分別可得到

$$w \equiv b \pmod{v} \Longrightarrow x = \alpha_w(n) \equiv \alpha_b(n) \pmod{v}; \tag{3.24}$$

$$w \equiv 2 \pmod{u} \Longrightarrow x = \alpha_w(n) \equiv \alpha_2(n) = n \pmod{u}. \tag{3.25}$$

令

$$n = 2lm \pm j,\ \ j \leq m. \tag{3.26}$$

由 (3.1) 可得到

$$\begin{aligned} A_b(n) &= E_b^n \\ &= E_b^{2lm \pm j} \\ &= \left((E_b^m)^2\right)^l E_b^{\pm j} \\ &= \left((A_b(m))^2\right)^l A_b(j)^{\pm 1}. \end{aligned} \tag{3.27}$$

由 (3.21) 可知

$$\begin{aligned} A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ &\equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m-1) \end{pmatrix} \pmod{v} \\ &\equiv -A_b(m)^{-1} \pmod{v}, \end{aligned}$$

因此

$$A_b(m)^2 \equiv -E \pmod{v}. \tag{3.28}$$

由 (3.27), (3.28) 可知

$$A_b(n) \equiv \pm A_b(j)^{\pm 1} \pmod{v}. \tag{3.29}$$

由 (3.24), (3.29) 及 $\det A_b(j) = 1$ 得到

$$x \equiv \alpha_b(n) \equiv \pm\alpha_b(j) \pmod{v}. \tag{3.30}$$

由 (3.26), (3.6), (3.11) 及 (3.20) 可知

$$2\alpha_b(j) \le 2\alpha_b(m) \le (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v. \tag{3.31}$$

由 (3.17), (3.23), (3.24), (3.30) 及 (3.31) 我們得到

$$a = \mathrm{arem}(x, v) = \mathrm{arem}(\alpha_b(n), v) = \alpha_b(j). \tag{3.32}$$

再由 (3.16) 及 (3.32) 我們得到

$$2j \le 2\alpha_b(j) = 2a < u. \tag{3.33}$$

從 (3.18), (3.22), (3.25) 及 (3.26) 得到

$$c = \mathrm{arem}(x, u) = \mathrm{arem}(n, u) = j. \tag{3.34}$$

由 (3.32) 及 (3.34) 可推得 $a = \alpha_b(c)$。

反之，若 $a = \alpha_b(c), b \ge 4, c \ge 0$，我們要證明存在非負整數 u, t, s, r, v, w, x 與 y 使方程組 (3.6) $\sim$ (3.18) 成立。先取

$$u = \alpha_b(k), t = \alpha_b(k+1),$$

其中 $k \in N, u > 2a$，且 u 為奇數（此時滿足條件 (3.7), (3.16)）。

再取 $m = uk$ 及

$$s = \alpha_b(m), r = \alpha_b(m-1) \ , m = uk,$$

此時滿足 (3.8)。由 (3.5) 知

$$s = \alpha_b(uk) \equiv (-1)^{u-1} u\alpha_b(k)\alpha_b^{u-1}(k-1) \pmod{u^2}.$$

故 $u^2|s$（滿足條件 (3.10)）。取 $v = bs - 2r$（滿足條件 (3.11)），若 $d|u, d|v$，則 $d|s, d|2r$。因為 u 為奇數，所以 d 亦為奇數，因此 $d|r$。又因為 $s = \alpha_b(m), r = \alpha_b(m-1)$ 互質，所以 $d = 1$，即 u, v 互質。

由中國剩餘定理，我們知道存在 w 滿足條件 $(3.12), (3.13), (3.14)$。令

$$x = \alpha_w(c), y = \alpha_w(c+1).$$

此時滿足條件 (3.15)。由 (3.12) 我們有

$$x = \alpha_w(c) \equiv \alpha_b(c) = a \pmod{v},$$

又由 (3.11) 得到

$$v = bs - 2r > 4\alpha_b(m) - 2\alpha_b(m-1) > 2\alpha_b(m) = 2\alpha_b(uk) > \alpha_b(k) = u > 2a,$$

所以

$$a = \mathrm{arem}(x, v),$$

此時滿足條件 (3.17)。又

$$x = \alpha_w(c) \equiv \alpha_2(c) = c \pmod{w-2},$$

$$x \equiv c \pmod{u}\text{（利用}(3.13)\text{）},$$

$$2c \leq 2\alpha_b(c) = 2a < u,$$

所以

$$c = \mathrm{arem}(x, u)$$

此時滿足條件 (3.18)。所以 $(3.6) \sim (3.18)$ 皆成立。 ⊠

定理 **3.5** 若定義 $0^0 = 1$, 則冪函數 $f(b, c) = b^c$（定義域為 N^2）是刁藩圖函數。即集合 $\{(a, b, c) \in N^3 | a = b^c\}$ 是一個刁藩圖集。

〔證明〕若 $b \geq 2$, 則對 n 作數學歸納法可知

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n.$$

對任意非負整數 $x > 4$，利用上式得到

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \geq \frac{(bx+3)^c}{x^c} \geq b^c.$$

若 $c = 0$ 時，則

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = 1 = b^c.$$

若 $b = 0, c > 0$ 時，則

$$0 < \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} < \frac{4^c}{(x-1)^c} \leq 1.$$

因此在 $b = 0$ 或 $c = 0$ 時，恆有

$$b^c = \alpha_{bx+4}(c+1) \text{ div } \alpha_x(c+1).$$

若 $b \geq 1, c \geq 1$ 且 $x > 16c$ 時，則

$$\begin{aligned}
\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} &\leq \frac{(bx+4)^c}{(x-1)^c} \\
&\leq \frac{(1+4/x)^c}{(1-1/x)^c} b^c \\
&\leq \frac{b^c}{(1-1/x)^c(1-4/x)^c} \\
&\leq \frac{b^c}{(1-4/x)^{2c}} \\
&\leq \frac{b^c}{1-\frac{8c}{x}} \\
&\leq b^c\left(1+\frac{16c}{x}\right).
\end{aligned}$$

當 $x > 16(c+1)(b+1)^c$ 時，

$$b^c \leq b^c\left(1+\frac{16c}{x}\right) < b^c + 1,$$

即

$$\alpha_{bx+4}(c+1) \text{ div } \alpha_x(c+1) = b^c.$$

當我們取

$$x = 16(c+1)\alpha_{b+4}(c+1)$$

時，則

$$b^c = \alpha_{bx+4}(c+1) \text{ div } \alpha_x(c+1).$$

因為函數 $b \text{ div } c, \alpha_b(c)$ 是刁藩圖的，所以函數 b^c 是刁藩圖的。 ⊠

對任意非負整數 a，以正整數 $b \geq 2$ 為底， a 的展開式為

$$a = a_{n+1}b^n + a_n b^{n-1} + \cdots + a_2 b^1 + a_1 b^0,$$

其中

$$0 \leq a_i < b, i = 1, \cdots, n+1.$$

我們用符號 $\text{Elem}(a, b, k+1)$ 代表展開式中 b^k 項的係數，也就是 a_{k+1}。因為

$$e = \text{Elem}(a, b, k+1) \Longleftrightarrow \exists x, y$$

$$[a = xb^{k+1} + eb^k + y \bigwedge e < b \bigwedge y < b^k].$$

所以函數 $\text{Elem}(a, b, k+1)$ 是一個刁藩圖函數。

定理 **3.6** 若規定

$$\binom{0}{m} = \begin{cases} 1 & m = 0, \\ 0 & m \geq 1, \end{cases}$$

則函數 $f(n, m) = \binom{n}{m}$ 是一個刁藩圖函數（定義域為 N^2）。

〔證明〕已知

$$(b+1)^n = \sum_{i=0}^{n} \binom{n}{i} b^i.$$

因為 $\binom{n}{i} < 2^n + 1 (0 \le i \le n)$，所以

$$c = \binom{n}{m} \Longleftrightarrow c = \mathrm{Elem}((2^n+2)^n, 2^n+1, m+1).$$

故函數 $f(n,m) = \binom{n}{m}$ 是一個刁藩圖函數。 ⊠

定理 **3.7** 若規定 $0! = 1$，則函數 $f(m) = m!$ 是一個刁藩圖函數。

〔證明〕當 $n \ge m \ge 0$ 時，

$$\begin{aligned} m! &= \frac{n!}{\binom{n}{m}(n-m)!} \\ &= \frac{n(n-1)\cdots(n-m+1)}{\binom{n}{m}} \\ &= \frac{n^m}{\binom{n}{m}} \left(1-\frac{1}{n}\right)\cdots\left(1-\frac{m-1}{n}\right) \\ &= \lim_{n\to\infty} \frac{n^m}{\binom{n}{m}} \left(1-\frac{1}{n}\right)\cdots\left(1-\frac{m-1}{n}\right) \\ &= \lim_{n\to\infty} \frac{n^m}{\binom{n}{m}}, \end{aligned}$$

所以數列

$$a(n) = \frac{n^m}{\binom{n}{m}}$$

是一個收斂至 $m!$ 的遞減數列。若 n 夠大時，可得到

$$m! \le \frac{n^m}{\binom{n}{m}} < m! + 1$$

即

$$m! = n^m \mathrm{div} \binom{n}{m}.$$

取 $n = (m+1)^{m+2}$，則

$$m! = (m+1)^{m(m+2)} \mathrm{div} \binom{(m+1)^{m+2}}{m}.$$

因此函數 $f(m) = m!$ 是一個刁藩圖函數，得證。 ⊠

定理 **3.8** 質數所構成的集合是一個刁藩圖集。

〔證明〕我們以 $\mathrm{Prime}(a)$ 代表 a 是一個質數。因為

$$\mathrm{Prime}(a) \Longleftrightarrow a > 1 \bigwedge \gcd(a, (a-1)!) = 1.$$

由以上關係式可知，質數所構成的集合是一個刁藩圖集。 ⊠

3.3 幾個特殊的刁藩圖敘述

設 $P(x_1,\cdots,x_n)$ 是一個關於序對 $(x_1,\cdots,x_n)\in N^n$ 的敘述，若集合

$$D=\{(x_1,\cdots,x_n)\in N^n|\text{敘述}P(x_1,\cdots,x_n)\text{成立}\}$$

是刁藩圖的，則稱敘述 $P(x_1,\cdots,x_n)$ 是刁藩圖的。設

$$a_1,\cdots,a_n\in N \tag{3.35}$$

是一個有限數列，我們可找到三元序對 (a,b,c) 來代表這個數列，其中

$$c=n, \tag{3.36}$$

$$b>a_i, i=1,\cdots,n, \tag{3.37}$$

$$a=a_nb^{n-1}+\cdots+a_1b^0. \tag{3.38}$$

若三元序對 (a,b,c) 滿足條件 (3.36), (3.37) 及 (3.38)，則 (a,b,c) 可唯一決定數列 (3.35)，因此我們稱 (a,b,c) 是數列 (3.35) 的 位置碼 (positionalcode)。由位置碼的取法我們知道：一個有限數列可對應無限多個位置碼，但一個位置碼僅對應唯一的一個有限數列。並非任意三元序對都是位置碼，也就是說，任意三元序對不一定能對應到一個有限數列，它必須滿足以下條件：

$$b\geq 2\bigwedge a<b^c, \tag{3.39}$$

我們以 $\text{Code}(a,b,c)$ 來表示滿足敘述 (3.39) 的三元序對 (a,b,c)，由表示法可知，敘述 $\text{Code}(a,b,c)$ 是刁藩圖的。

若位置碼 (a_1,b_1,c_1) 與 (a_2,b_2,c_2) 皆對應相同的一個有限數列，則我們以敘述

$$\text{Equal}(a_1,b_1,c_1,a_2,b_2,c_2)$$

來表示，我們將證明敘述 $\text{Equal}(a_1,b_1,c_1,a_2,b_2,c_2)$ 是刁藩圖的。另外敘述 $\text{NotGreater}(a_1,b_1,a_2,b_2)$ 與 $\text{Small}(a,b,c,e)$ 分別定義如下：

$$\begin{aligned}\text{NotGreater}(a_1,b_1,a_2,b_2) &\iff \forall k\geq 1[\text{Elem}(a_1,b_1,k)\leq\text{Elem}(a_2,b_2,k)],\\ \text{Small}(a,b,c,e) &\iff \text{Code}(a,b,c)\bigvee\forall k\geq 1[\text{Elem}(a,b,k)\leq e].\end{aligned}$$

其表示法皆包含 $\forall k$ 的描述，因此仍無法判別敘述 $\text{NotGreater}(a_1,b_1,a_2,b_2)$ 與 $\text{Small}(a,b,c,e)$ 是否是刁藩圖的，在證明以下幾個敘述之後，我們將得到肯定的答案。

敘述 $\text{PNotGreater}(a_1,a_2,b)$ 定義如下：

$$\text{PNotGreater}(a_1,a_2,b)\iff\text{Prime}(b)\bigwedge\text{NotGreater}(a_1,b,a_2,b).$$

設 b 是一個質數，因為

$$\binom{m+n}{m}=\frac{(m+n)!}{m!n!},$$

所以

$$\deg_b\binom{m+n}{m}=\deg_b(m+n)!-\deg_bm!-\deg_bn!,$$

其中 $\deg_b k$ 代表 k 的質因數分解中 b 的次數。我們可得到

$$\deg_b k! = \sum_{i\geq 1} k \text{ div } b^i.$$

設

$$a_2 \geq a_1,$$
$$a_1 = k_c b^{c-1} + \cdots + k_1 b^0,$$
$$a_2 - a_1 = k'_c b^{c-1} + \cdots + k'_1 b^0,$$

其中 $0 \leq k'_i, k_i < b, i = 1, \cdots, c.$ 若 $0 \leq k_i + k'_i < b, i = 1 \cdots, c,$ 也就是說，若 $(a_1, b, a_2, b) \in \text{NotGreater}(a_1, b, a_2, b)$ 則

$$\begin{aligned}
\deg_b \binom{a_2}{a_1} &= \deg_b a_2! - \deg_b a_1! - \deg_b (a_2 - a_1)! \\
&= \sum_{j=1}^{c-1} \left(a_2 \text{ div } b^j - a_1 \text{ div } b^j - (a_2 - a_1) \text{ div } b^j\right) \\
&= 0.
\end{aligned}$$

若存在一個 i 使得 $b \leq k_i + k'_i < 2b,$ 則

$$(k_i + k'_i) b^{i-1} \text{ div } b^j = k_i b^{i-1} \text{ div } b^j + k'_i b^{i-1} \text{ div } b^j, j \neq i,$$

但是

$$(k_i + k'_i) b^{i-1} \text{ div } b^i = k_i b^{i-1} \text{ div } b^i + k'_i b^{i-1} \text{ div } b^i + 1 = 1.$$

因此若 $(a_1, b, a_2, b) \notin \text{NotGreater}(a_1, b, a_2, b),$ 則

$$\begin{aligned}
\deg_b \binom{a_2}{a_1} &= \sum_{j=1}^{c-1} \left(a_2 \text{ div } b^j - a_1 \text{ div } b^j - (a_2 - a_1) \text{ div } b^j\right) \\
&\geq \sum_{j=1}^{c-1} \sum_{l=1}^{c} \left((k_l + k'_l) b^{l-1} \text{ div } b^j - k_l b^{l-1} \text{ div } b^j - k'_l b^{l-1} \text{ div } b^j\right) \\
&\geq \sum_{j=1}^{c-1} \left((k_i + k'_i) b^{i-1} \text{ div } b^j - k_i b^{i-1} \text{ div } b^j - k'_i b^{i-1} \text{ div } b^j\right) \\
&= (k_i + k'_i) b^{i-1} \text{ div } b^i - k_i b^{i-1} \text{ div } b^i - k'_i b^{i-1} \text{ div } b^i = 1.
\end{aligned}$$

因此 (a_1, b, a_2, b) 滿足敘述 $\text{NotGreater}(a_1, b, a_2, b)$ 的充份必要條件為：

$$\deg_b \binom{a_2}{a_1} = 0,$$

即

$$b \not| \binom{a_2}{a_1}.$$

因此

$$\mathrm{PNotGreater}(a_1, a_2, b) \Longleftrightarrow \mathrm{Prime}(b) \bigwedge b \not| \binom{a_2}{a_1}.$$

由表示法可知，敘述 $\mathrm{PNotGreater}(a_1, a_2, b)$ 是刁藩圖的。

敘述 $\mathrm{PSmall}(a, b, c, e)$ 定義如下：

$$\begin{aligned} \mathrm{PSmall}(a, b, c, e) &\Longleftrightarrow \mathrm{Prime}(b) \bigwedge \mathrm{Small}(a, b, c, e) \\ &\Longleftrightarrow \mathrm{Prime}(b) \bigwedge [e \geq b \bigvee \mathrm{PNotGreater}(a, \mathrm{Repeat}(e, b, c), b)]. \end{aligned}$$

其中 $\mathrm{Repeat}(e, b, c) = e(b^c - 1)/(b - 1)$。若 $e < b$，則 $(\mathrm{Repeat}(e, b, c), b, c)$ 是 c 個 e 所構成的數列所對應的位置碼。由表示法可知，敘述 $\mathrm{PSmall}(a, b, c, e)$ 是刁藩圖的。

敘述 $\mathrm{Eq}(a_1, b_1, c_1, a_2, b_2, c_2)$ 定義如下：

$$\begin{aligned} &\mathrm{Eq}(a_1, b_1, c_1, a_2, b_2, c_2) \Longleftrightarrow \mathrm{Code}(a_1, b_1, c_1) \bigwedge c_1 = c_2 \\ &\quad \bigwedge \mathrm{PSmall}(a_2, b_2, c_2, b_1 - 1) \bigwedge b_1^{c_1} + b_1 < b_2 \bigwedge a_1 \equiv a_2 \pmod{b_2 - b_1}. \end{aligned}$$

由表示法可知，敘述 $\mathrm{Eq}(a_1, b_1, c_1, a_2, b_2, c_2)$ 是刁藩圖的。若 b_1, a_2, b_2 之值確定，且滿足

$$a_1 \equiv a_2 \pmod{b_2 - b_1},$$

$$a_1 < b_1^{c_1} < b_2 - b_1,$$

則 a_1 之值必唯一確定。也就是說，若 $(a_1, b_1, c_1, a_2, b_2, c_2)$ 滿足敘述

$$\mathrm{Eq}(a_1, b_1, c_1, a_2, b_2, c_2)$$

，則位置碼 $\mathrm{Code}(a_1, b_1, c_1)$ 與 $\mathrm{Code}(a_2, b_2, c_2)$ 所對應的數列必相同。我們可利用敘述 Eq 來表示敘述 Equal 如下：

$$\begin{aligned} &\mathrm{Equal}(a_1, b_1, c_1, a_2, b_2, c_2) \Longleftrightarrow \\ &\qquad \exists x, y, z[\mathrm{Eq}(a_1, b_1, c_1, x, y, z)] \bigwedge \mathrm{Eq}(a_2, b_2, c_2, x, y, z)]. \end{aligned}$$

所以敘述 $\mathrm{Equal}(a_1, b_1, c_1 a_2, b_2, c_2)$ 是刁藩圖的。同理，利用以上的刁藩圖敘述我們得到：

$$\begin{aligned} &\mathrm{NotGreater}(a_1, b_1, a_2, b_2) \Longleftrightarrow \exists x_1, x_2, y, z[\mathrm{Equal}(a_1, b_1, z, x_1, y, z) \\ &\quad \bigwedge \mathrm{Equal}(a_2, b_2, z, x_2, y, z) \bigwedge \mathrm{PNotGreater}(x_1, x_2, y)], \end{aligned}$$

$$\mathrm{Small}(a, b, c, e) \Longleftrightarrow \exists x, y[\mathrm{Equal}(a, b, c, x, y, c) \bigwedge \mathrm{PSmall}(x, y, c, e)].$$

因此敘述 $\mathrm{NotGreater}(a_1, b_1, a_2, b_2)$ 與 $\mathrm{Small}(a, b, c, e)$ 也是刁藩圖的。令敘述 $\mathrm{SCod}(d, m, f, g, h)$ 與 $\mathrm{Solution}(a, b, c_L, c_R, d, m, f, g, h)$ 定義如下：

$$\begin{aligned} &\mathrm{SCod}(d, m, f, g, h) \Longleftrightarrow \\ &\qquad \exists s[\mathrm{Equal}(f, 2, d^m + 1, s, g, d^m + 1) \bigwedge \mathrm{NotGreater}(h, g, (g - 1)s, g)]. \end{aligned}$$

$$\begin{aligned}\mathrm{Solution}(a,b,c_L,c_R,d,m,f,g,h) \Longleftrightarrow \exists s_L,s_R,t,w[\\ &\mathrm{SCod}(d,m,f,g,h)\\ &\bigwedge w > (1+a+h)^{d-1}(c_L+c_R)\\ &\bigwedge \mathrm{Equal}(h,g,d^m+1,t,w,d^m+1)\\ &\bigwedge \mathrm{Equal}(c_L,b,d^{m+1}+1,s_L,w,d^{m+1}+1)\\ &\bigwedge \mathrm{Equal}(c_R,b,d^{m+1}+1,s_R,w,d^{m+1}+1)\\ &\bigwedge \mathrm{Elem}((1+aw+t)^{d-1}s_L,w,d^{m+1}+1)\\ &\quad = \mathrm{Elem}((1+aw+t)^{d-1}s_R,w,d^{m+1}+1)].\end{aligned}$$

由表示法可知，敘述 $\mathrm{SCod}(d,m,f,g,h)$ 與 $\mathrm{Solution}(a,b,c_L,c_R,d,m,f,g,h)$ 都是刁藩圖的，利用這些敘述我們可在下一節證明存在通用刁藩圖方程式。

3.4 通用刁藩圖方程式

在這一節中，我們先證明存在“通用刁藩圖方程式”，再利用通用方程式證明存在一個一維度的刁藩圖集，其餘集不是刁藩圖集。

所謂“通用刁藩圖方程式”是指一個變數為

$$a_1,\cdots,a_n,k_1,\cdots,k_l,y_1,\cdots,y_w$$

的刁藩圖方程式

$$U(a_1,\cdots,a_n,k_1,\cdots,k_l,y_1,\cdots,y_w)=0$$

滿足：對任意 n 個參數的刁藩圖方程式

$$D(a_1,\cdots,a_n,x_1,\cdots,x_m)=0,$$

存在一個非負整數序對 $(k_1^D,\cdots,k_l^D)$，使得方程式

$$U(a_1,\cdots,a_n,k_1^D,\cdots,k_l^D,y_1,\cdots,y_w)=0$$

所生成的刁藩圖集與方程式 D 所產生的刁藩圖集 S 相同。換句話說，方程式

$$U(a_1,\cdots,a_n,k_1^D,\cdots,k_l^D,y_1,\cdots,y_w)=0$$

是刁藩圖集 S 的另一個刁藩圖表現。稱變數 $a_1,\cdots,a_n$ 為參數， $k_1,\cdots,k_l$ 為參數碼， $y_1,\cdots,y_w$ 為未知數。

函數

$$(a,b)\mapsto \mathrm{Cantor}_2(a,b)=\frac{(a+b)^2+3a+b}{2}.$$

是一個從 N^2 一對一映成至 N 的函數。我們定義 $\mathrm{Cantor}_{n+1}(n\geq 2)$ 為

$$\mathrm{Cantor}_{n+1}(a_1,\cdots,a_{n+1}) \;=\; \mathrm{Cantor}_n(a_1,\cdots,a_{n-1},\mathrm{Cantor}_2(a_n,a_{n+1})),$$

則 Cantor_{n+1} 是一個 N^{n+1} 一對一映成至 N 的函數。因為表示法

$$\mathrm{Cantor}_n(a_1,\cdots,a_n)$$

展開的多項式中係數並非整數，因此乘上 2^{2^n} 後，多項式

$$2^{2^n}\mathrm{Cantor}_n(a_1,\cdots,a_n)$$

的係數為整數。

利用上述的結果，我們將證明對任意一個通用刁藩圖方程式

$$U(a_1,\cdots,a_n,k_1,\cdots,k_l,y_1,\cdots,y_w)=0,$$

皆可轉換成 1 個參數碼， $l+w$ 個未知數的通用刁藩圖方程式。

定理 **3.9** 若方程式

$$U(a_1,\cdots,a_n,k_1,\cdots,k_l,y_1,\cdots,y_w)=0$$

是 l 個參數碼的通用刁藩圖方程式，則

$$U^2(a_1,\cdots,a_n,k_1,\cdots,k_l,y_1,\cdots,y_w)+(k-2^{2^l}\mathrm{Cantor}_l(k_1,\cdots,k_l))^2=0$$

是 1 個參數碼指 k， $l+w$ 未知數指 $k_1,\cdots,k_l,y_1,\cdots,y_w$ 的通用刁藩圖方程式。

〔證明〕令方程式

$$\begin{aligned}&U^{'}(a_1,\cdots,a_n,k,k_1,\cdots,k_l,y_1,\cdots,y_w)\\&\quad=U^2(a_1,\cdots,a_n,k_1,\cdots,k_l,y_1,\cdots,y_w)+(k-2^{2^l}\mathrm{Cantor}_l(k_1,\cdots,k_l))^2=0.\end{aligned}$$

很容易可檢驗出當 $k_1^D,\ldots,k_l^D$ 代入 U 所得的刁藩圖集與

$$k^D=2^{2^l}\mathrm{Cantor}_l(k_1^D,\cdots,k_l^D)$$

代入 U' 所得的刁藩圖集相同。因此 U' 亦為通用刁藩圖方程式。 ⊠

我們將證明對任意 $n\geq 1$，存在 n 個參數的通用刁藩圖方程式。

定理 **3.10** 若存在一個參數的通用刁藩圖方程式

$$U_1(a,k,y_1,\cdots,y_w)=0,$$

則對任意正整數 n，必存在 n 個參數的通用刁藩圖方程式。

〔證明〕我們將證明方程式

$$U_n(a_1,\cdots,a_n,k,y_1,\cdots,y_w)=U_1(2^{2^n}\mathrm{Cantor}_n(a_1,\cdots,a_n),k,y_1,\cdots,y_w)=0$$

是 n 個參數的通用刁藩圖方程式。設刁藩圖方程式

$$D(a_1,\cdots,a_n,x_1,\cdots,x_m)=0$$

所生成的刁藩圖集為 S_n, 則方程式

$$D^2(a_1,\cdots,a_n,x_1,\cdots,x_m)+(a-2^{2n}\mathrm{Cantor}_n(a_1,\cdots,a_n))^2=0$$

是刁藩圖集

$$S_1 = \{a = 2^{2^n}\mathrm{Cantor}_n(a_1, \cdots, a_n) | (a_1, \cdots, a_n) \in S_n\}$$

的刁藩圖表現。已知存在一個參數碼 k^D，使得方程式

$$U_1(a, k^D, y_1, \cdots, y_w) = 0$$

也是刁藩圖集 S_1 的刁藩圖表現。由 $U_n(a_1, \cdots, a_n, k, y_1, \cdots, y_w) = 0$ 的定義容易推得：$U_n(a_1, \cdots, a_n, k^D, y_1, \cdots, y_m) = 0$ 的刁藩圖集為 S_n，故

$$U(a_1, \cdots, a_n, k, y_1, \cdots, y_m) = 0$$

是 n 個參數的通用刁藩圖方程式。 ⊠

定理 **3.11** 存在 1 個參數的通用刁藩圖方程式。

〔證明〕設

$$D(a, x_1, \cdots, x_m) = 0$$

是 1 個參數的刁藩圖方程式，我們可將方程式 $D = 0$ 移項成為

$$C_L(a, x_1, \cdots, x_m) = C_R(a, x_1, \cdots, x_m),$$

使得多項式 C_L, C_R 的係數為非負整數。令多項式 C_L, C_R 如下：

$$C_L(a, x_1, \cdots, x_m) = \sum_{i_0+\cdots+i_m<d} c_{L,i_0,\cdots,i_m} a^{i_0} x_1^{i_1} \cdots x_m^{i_m},$$

$$C_R(a, x_1, \cdots, x_m) = \sum_{i_0+\cdots+i_m<d} c_{R,i_0,\cdots,i_m} a^{i_0} x_1^{i_1} \cdots x_m^{i_m}.$$

針對方程式 $D = 0$, 我們設定一組六元序對 (b, c_L, c_R, d, m, f) 如下：

$$d > \text{方程式的次數}. \tag{3.40}$$

$$m = \text{未知數的個數}, \tag{3.41}$$

$$f = 2^{d^1} + \cdots + 2^{d^m}, \tag{3.42}$$

$$c_L = \sum_{i_0+\cdots+i_m<d} i_0! \cdots i_m! (d-1-i_0-\cdots-i_m)! c_{L,i_0,\cdots,i_m} b^{d^{m+1}-i_0 d^0-\cdots-i_m d^m}, \tag{3.43}$$

$$c_R = \sum_{i_0+\cdots+i_m<d} i_0! \cdots i_m! (d-1-i_0-\cdots-i_m)! c_{R,i_0,\cdots,i_m} b^{d^{m+1}-i_0 d^0-\cdots-i_m d^m}, \tag{3.44}$$

$$b > d! \max\{c_{L,i_0,\cdots,i_m}, c_{R,i_0,\cdots,i_m}\}. \tag{3.45}$$

從設定的過程中可以發現：六元序對 (b, c_L, c_R, d, m, f) 的設定不是唯一的 (其中 m 是唯一的)；但是，如果 (b, c_L, c_R, d, m, f) 滿足條件 (3.40) ∼ (3.45), 則 (b, c_L, c_R, d, m, f) 對應的方程式是唯一的。因此我們稱滿足條件 (3.40) ∼ (3.45) 的六元序對 (b, c_L, c_R, d, m, f) 為 擴展碼 (extended code)，通常我們用 $D_{b,c_L,c_R,d,m,f} = 0$ 取代方程式 $D = 0$。

底下我們將證明存在 1 個參數， 6 個參數碼的通用刁藩圖方程式

$$U(a, b, c_L, c_R, d, m, f, y_7, \cdots, y_l) = 0.$$

首先證明： $(a, x_1, \cdots, x_m)$ 為方程式

$$D_{b,c_L,c_R,d,m,f}(a, x_1, \cdots, x_m) = 0 \tag{3.46}$$

的一個非負整數解的充份必要條件為關係式 (3.47) $\sim$ (3.53) 成立：
存在 $(g, h, w, t, s_L, s_R) \in N^6$ 使得

$$g > 1, g > x_1, \cdots, g > x_m, \tag{3.47}$$

$$h = x_1 g^{d^1} + x_2 g^{d^2} + x_m g^{d^m}, \tag{3.48}$$

$$w > (1 + a + h)^{d-1}(c_L + c_R), \tag{3.49}$$

$$t = x_1 w^{d^1} + \cdots + x_m w^{d^m}, \tag{3.50}$$

$$s_L = \sum_{i_0+\cdots+i_m<d} i_0! \cdots i_m!(d-1-i_0-\cdots-i_m)! c_{L,i_0,\cdots,i_m} w^{d^{m+1}-i_0 d^0-\cdots-i_m d^m}, \tag{3.51}$$

$$s_R = \sum_{i_0+\cdots+i_m<d} i_0! \cdots i_m!(d-1-i_0-\cdots-i_m)! c_{R,i_0,\cdots,i_m} w^{d^{m+1}-i_0 d^0-\cdots-i_m d^m}, \tag{3.52}$$

$$\mathrm{Elem}((1+aw+t)^{d-1} s_L, w, d^{m+1}+1)) = \mathrm{Elem}((1+aw+t)^{d-1} s_R, w, d^{m+1}+1)). \tag{3.53}$$

若 $(a, x_1, \cdots, x_m)$ 滿足 (3.47) $\sim$ (3.53)，則利用 (3.50) 得到

$$\begin{aligned}(1+aw+t)^{d-1} &= (1 + aw^{d^0} + x_1 w^{d^1} + x_2 w^{d^2} + \cdots + x_m w^{d^m})^{d-1} \\ &= \sum_{i_0+\cdots+i_m<d} \binom{d-1}{i_0, \cdots, i_m} a^{i_0} x_1^{i_1} \cdots x_m^{i_m} w^{i_0 d^0 + \cdots + i_m d^m}.\end{aligned}$$

我們可將 $(1+aw+t)^{d-1} s_L$ 表示成

$$(1+aw+t)^{d-1} s_L = \sum_{k=0}^{2d^{m+1}-1} C_{L,k} w^k, \tag{3.54}$$

其中 $C_{L,k}$ 是以 $c_{L,i_0\cdots i_m}, a, x_1, \cdots, x_m$ 為變數的多項式，並可得出

$$\begin{aligned}C_{L,d^{m+1}} &= \sum_{i_0+\cdots+i_m<d} (d-1)! c_{L,i_0,\cdots,i_m} a^{i_0} x_1^{i_1} \cdots x_m^{i_m} \\ &= (d-1)! C_L(a, x_1, \cdots, x_m).\end{aligned}$$

由 (3.54) 以 1 取代 w 及 (3.49) 可知

$$w > C_{L,0}, \cdots, C_{L,2d^{m+1}-1}.$$

所以

$$C_L(a, x_1, \cdots, x_m) = \frac{\mathrm{Elem}\left((1+aw+t)^{d-1} s_L, w, d^{m+1}+1\right)}{(d-1)!},$$

同理可得

$$C_R(a,x_1,\cdots,x_m)=\frac{\mathrm{Elem}\left((1+aw+t)^{d-1}s_R,w,d^{m+1}+1\right)}{(d-1)!}.$$

由條件 (3.53) 可知

$$C_L(a,x_1,\cdots,x_m)=C_R(a,x_1,\cdots,x_m),$$

即 $(a,x_1,\cdots,x_n)$ 是方程式 $D_{b,c_L,c_R,d,m,f}(a,x_1,\cdots,x_m)=0$ 的一組解。
反之，若 $(a,x_1,\cdots,x_m)$ 是方程式 $D_{b,c_L,c_R,d,m,f}=0$ 的解，很容易可找到 $(g,h,w,t,s_L,s_R)\in N^6$ 使方程式 (3.47) $\sim$ (3.53) 成立。

由以上的討論可知，當擴展碼 (b,c_L,c_R,d,m,f) 確定時，則條件 (3.47) $\sim$ (3.53) 所生成的一維刁藩圖集與方程式 $D_{b,c_L,c_R,d,m,f}=0$ 相同，但我們仍無法由條件 (3.47) $\sim$ (3.53) 造出一個通用刁藩圖方程式（因為對不同的刁藩圖方程式，d,m 的值可能是不同的）。但比較刁藩圖敘述：
$\mathrm{Solution}(a,b,c_L,c_R,d,m,f,g,h)\Longleftrightarrow\exists s_L,s_R,t,w[$

$$\begin{aligned}
&\mathrm{SCod}(d,m,f,g,h) && (3.55)\\
&\bigwedge w>(1+a+h)^{d-1}(c_L+c_R) && (3.56)\\
&\bigwedge \mathrm{Equal}(h,g,d^m+1,t,w,d^m+1) && (3.57)\\
&\bigwedge \mathrm{Equal}(c_L,b,d^{m+1}+1,s_L,w,d^{m+1}+1) && (3.58)\\
&\bigwedge \mathrm{Equal}(c_R,b,d^{m+1}+1,s_R,w,d^{m+1}+1) && (3.59)\\
&\bigwedge \mathrm{Elem}((1+aw+t)^{d-1}s_L,w,d^{m+1}+1) && (3.60)\\
&\quad=\mathrm{Elem}((1+aw+t)^{d-1}s_R,w,d^{m+1}+1)].
\end{aligned}$$

與條件 (3.47) $\sim$ (3.53) 可知：當 (b,c_L,c_R,d,m,f) 是一組給定的擴展碼時，因為

$$f=2^{d^1}+\cdots+2^{d^m},$$

所以條件 (1.54) 與 (3.47), (3.48) 是等價的；又 (1.55) $\sim$ (1.59) 分別等價於 (3.49) $\sim$ (3.53)。令

$$U(a,b,c_L,c_R,d,m,f,g,h,y_9,\cdots,y_l)=0 \tag{3.61}$$

是刁藩圖敘述 $\mathrm{Solution}(a,b,c_L,c_R,d,m,f,g,h)$ 的刁藩圖表現，其中 a 為參數，b,c_L,c_R,d,m,f 為參數碼，$g,h,y_9,\cdots,y_l$ 為未知數，則方程式 (3.61) 在參數碼以 (b,c_L,c_R,d,m,f) 代入所生成的一維刁藩圖集與方程式 $D_{b,c_L,c_R,d,m,f}=0$ 相同，因此 (3.61) 是一個參數的通用刁藩圖方程式。 ⊠

定理 **3.12** 存在一個一維的刁藩圖集 S，其餘集 $N-S$ 卻不是刁藩圖集。

〔證明〕由定理 3.9 及定理 3.11 可知：存在 1 個參數，1 個參數碼的通用刁藩圖方程式

$$U(a,k,y_1,\cdots,y_m)=0.$$

令刁藩圖方程式

$$U(a,a,y_1,\cdots,y_m)=0.$$

所生成的 1 維刁藩圖集為 S。我們可證明集合 S 的非負整數的餘集 $N-S$ 不是一個刁藩圖集。

若集合 $N-S$ 是一個刁藩圖集，則存在一個參數碼 k'，使得方程式

$$U(a,k',x_1,\cdots,x_m)=0$$

是集合 $N-S$ 的一個刁藩圖表現。若 $k'\in S$，則方程式

$$U(k',k',y_1,\cdots,y_m)=0$$

有非負整數解。即 k' 屬於方程式 $U(a,k',y_1,\cdots,y_m)=0$ 所生成的刁藩圖集，所以 $k'\in N-S$，此與假設 $k'\in S$ 矛盾。

又若 $k'\in N-S$。因為 k' 不屬於 S，所以

$$U(k',k',y_1,\cdots,y_m)=0$$

無非負整數解，所以 k' 不屬於 $U(a,k',y_1,\cdots,y_m)=0$ 所生成的刁藩圖集中，即 k' 不屬於 $N-S$，因此 $k'\in S$，此與假設 $k'\in N-S$ 矛盾。故 $N-S$ 不是一個刁藩圖集。 ⊠

第 4 章

希爾伯特第十問題(Hilbert's tenth problem)

本章首先證明受囿量詞是刁藩圖的，再證明一個全函數是刁藩圖的充份必要條件為它是遞歸的。最後證出希爾伯特第十問題的否定性答案，即不可能找到一個演算法來判斷任意的刁藩圖方程式是否有整數解。

4.1 受囿量詞是刁藩圖的

定理 **4.1** 若規定

$$\prod_{k=1}^{0}(a+bk)=1,$$

則函數

$$h(a,b,y)=\prod_{k=1}^{y}(a+bk)$$

是刁藩圖的（定義域為 N^3）。

〔證明〕取 $M=b(a+by)^y+1$，則 $(M,b)=1$，且存在一個 $q\in N$ 使得同餘式 $bq\equiv a \pmod M$ 成立。當 $b>0,y>0$ 時，

$$\begin{aligned} b^y y!\binom{q+y}{y} &= b^y(q+y)(q+y-1)\cdots(q+1)\\ &= (bq+by)(bq+b(y-1))\cdots(bq+b)\\ &\equiv (a+by)(a+b(y-1))\cdots(a+b) \pmod M\\ &\equiv \prod_{k=1}^{y}(a+bk) \pmod M \end{aligned}$$

且

$$\prod_{k=1}^{y}(a+bk)<M,$$

所以

$$z=\prod_{k=1}^{y}(a+bk) \iff \exists M,p,q,t\Big[\Big(b>0\bigwedge M=b(a+by)^y+1\bigwedge bq=a+Mt \\ \bigwedge z<M\bigwedge z+Mp=b^y y!\binom{q+y}{y}\Big)\bigvee(z=a^y\bigwedge b=0)\Big].$$

已知函數 $x^y, y!, \binom{x}{y}$ 都是刁藩圖的，所以函數

$$h(a,b,y)=\prod_{k=1}^{y}(a+bk)$$

是刁藩圖的。 ⊠

設受囿量詞 $(\forall k)_{\le y}$ 代表 k 是任何不超過 y 的非負整數；$(\exists k)_{\le y}$ 代表存在一個不超過 y 的非負整數 k；同理，量詞 $(\exists k)_{>y}$ 代表存在一個大於 y 的整數 k。

定理 **4.2** 設整數 $u\ge 1$, 且整係數多項式

$$P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m), Q(y,u,x_1,\cdots,x_n)$$

滿足

(1) 對所有整數 $0\le y,x_1,\cdots,x_n$ 恆有

$$Q(y,u,x_1,\cdots,x_n)>u, Q(y,u,x_1,\cdots,x_n)>y,$$

(2) 若整數 $0\le k\le y$ 且整數 $0\le y_1,\cdots,y_m\le u$， 則對所有的 $(x_1,\cdots,x_n)\in N^n$ 恆有

$$|P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)|\le Q(y,u,x_1,\cdots,x_n).$$

則底下 (a) 與 (b) 的解集合 $(y,x_1,\cdots,x_n)\in N^n$ 是相同的。

$$(a)\quad (\forall k)_{\le y}(\exists y_1,\cdots,y_m)_{\le u}\Big[P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=0]$$

$$(b)\quad \exists c,t,(a_1,\cdots,a_m)_{>u},(y_1^{(0)},\cdots,y_m^{(0)})_{\le u} \\ \Big[P(y,0,x_1,\cdots,x_n,y_1^{(0)},\cdots,y_m^{(0)})=0 \\ \bigwedge t=Q(y,u,x_1,\cdots,x_n)! \\ \bigwedge(1+ct)=\prod_{k=1}^{y}(1+kt) \\ \bigwedge(1+ct)\Big|a_1\prod_{j=1}^{u}(a_1-j)\bigwedge\cdots\bigwedge(1+ct)\Big|a_m\prod_{j=1}^{u}(a_m-j) \\ \bigwedge P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)\equiv 0 \pmod{1+ct}\Big].$$

〔證明〕先證明 $(b)\Rightarrow(a)$：由 (b) 可知：我們僅需討論 $1\le k\le y$ 的情況。對每一個 $k=1,\cdots,y$，令 p_k 是 $1+kt$ 的一個質因數，並令 $y_i^{(k)}$ 是 a_i 被 $p_k(k=1,\cdots,y,i=1,\cdots,m)$ 除的餘數。我們將證明：$y_i^{(k)},(i=1,\cdots,m,1\le k\le y)$ 滿足

(1) $1\le y_i^{(k)}\le u$,

(2) $P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0$.

先證明 (1)：已知

$$p_k|(1+kt),(1+kt)|(1+ct),(1+ct)\Big|a_i\prod_{j=1}^{u}(a_i-j),i=1,\cdots,m,$$

即 p_k 整除

$$a_i\prod_{j=1}^{u}(a_i-j),i=1,\cdots,m.$$

因為 p_k 是質數，所以存在 $0\le j\le u$ 使得 $p_k|(a_i-j)$. 因此可令

$$j\equiv a_i\equiv y_i^{(k)}\pmod{p_k}.$$

由 $t=Q(y,u,x_1,\cdots,x_n)!$, $p_k|(1+kt)$ 可知 p_k,t 互質，且

$$p_k>Q(y,u,x_1,\cdots,x_n)>u\ge j,$$

由於 $y_i^{(k)}$ 是 a_i 被 p_k 除的餘數，所以

$$y_i^{(k)}=j.$$

即

$$0\le y_i^{(k)}\le u.$$

其次證明 (2)：因為

$$1+ct\equiv 1+kt\equiv 0\pmod{p_k},$$

$$k+kct\equiv c+kct\pmod{p_k},$$

所以

$$k\equiv c\pmod{p_k}.$$

又

$$y_i^{(k)}\equiv a_i\pmod{p_k},$$

所以

$$P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})\equiv P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)\equiv 0\pmod{p_k}.$$

又由已知得到

$$|P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})|\le Q(y,u,x_1,\cdots,x_n)<p_k,$$

所以

$$P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0.$$

證明 $(a)\Rightarrow(b)$：設對任意 $1\le k\le y$，存在 $y_1^{(k)},\cdots,y_m^{(k)}$ 使得

$$P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0,$$

$$0\le y_j^{(k)}\le u, j=1,\cdots,m.$$

令

$$t=Q(y,u,x_1,\cdots,x_n)!.$$

由於

$$\prod_{k=1}^{y}(1+kt)\equiv 1 \pmod{t},$$

所以存在整數 $c\ge 0$ 使得

$$1+ct=\prod_{k=1}^{y}(1+kt).$$

又當 $1\le k<l\le y$ 時

$$(1+kt,1+lt)=1,$$

這是因為令 $p|(1+kt),p|(1+lt),p>1$，於是 $p|(l-k),p<y$，但

$$Q(y,u,x_1,\cdots,x_n)>y,$$

於是 $p|t$, 矛盾。因此 $\{1+kt|k=1,\cdots,y\}$ 中兩兩互質，利用中國剩餘定理：對每個 $i,1\le i\le m$，存在 a_i 使得

$$\begin{aligned}&a_i\equiv y_i^{(k)} \pmod{1+kt}, k=1,\cdots,y,\\ &a_i>u, i=1,\cdots,m.\end{aligned}$$

由 $(1+kt)$ 整除 $c(1+kt)-k(1+ct)$ 可得 $k\equiv c \pmod{1+kt}$, 因此

$$\begin{aligned}&P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)\\ &\quad\equiv P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0 \pmod{1+kt}.\end{aligned}$$

又因為 $1+kt$ $(k=1,2,\cdots,y)$ 是兩兩互質的，且 $1+kt$ 整除

$$P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m), k=1,\cdots,y.$$

所以這些 $1+kt$ 的乘積也整除 $P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)$，即 $1+ct$ 整除

$$P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m).$$

又 $a_i\equiv y_i^{(k)} \pmod{1+kt}, k=1,\cdots,y$, 所以 $1+kt$ 整除

$$a_i-y_i^{(k)}.$$

因為 $0 \le y_i^{(k)} \le u$, 所以 $1+kt$ 整除

$$a_i\Big(\prod_{j=1}^{u}(a_i-j)\Big), i=1,\cdots,m.$$

又 $1+kt$ 彼此互質，所以 $1+ct$ 整除

$$a_i\Big(\prod_{j=1}^{u}(a_i-j)\Big), i=1,\cdots,m.$$

⊠

定理 **4.3** 若 P 是一個整係數多項式，則集合

$$S=\{(y,x_1,\cdots,x_n)\in N^{n+1} \mid (\forall k)_{\le y}\,\exists y_1,\cdots,y_m \\ [P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=0]\}$$

是刁藩圖的。也就是說，量詞 $(\forall k)_{\le y}$ 是刁藩圖的。

〔證明〕首先很容易觀察出以下等價式是成立的：

$$\begin{aligned} & (\forall k)_{\le y}\,\exists y_1,\cdots,y_m[P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=0] \\ \iff\ & \exists u\,(\forall k)_{\le y}(\exists y_1,\cdots,y_m)_{\le u}\,[P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=0]. \end{aligned}$$

由等價式的關係，我們可排除 $u=0$ 的情況。將多項式 P 表示如下：

$$P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=\sum_{a+b+q_1+\cdots+q_n+s_1+\cdots+s_m<N} cy^a k^b x_1^{q_1}\cdots x_n^{q_n}y_1^{s_1}\cdots y_m^{s_m}.$$

其中

$$N>\text{多項式}P\text{的次數}.$$

令多項式

$$Q(y,u,x_1,\cdots,x_n)=u+y+\sum_{a+b+q_1+\cdots+q_n+s_1+\cdots+s_m<N}|c|y^{a+b}x_1^{q_1}\cdots x_n^{q_n}u^{s_1+\cdots+s_m}.$$

則整係數多項式 Q 滿足定理 4.2 的條件。已知函數

$$\prod_{k=1}^{y}(1+kt),$$
$$\prod_{j=1}^{u}(a_i-j)=\prod_{j=1}^{u}(a_i-u-1+j)$$

都是刁藩圖的，由定理 4.2 的表示法可知，集合 S 是刁藩圖的，也就是量詞 $(\forall k)_{\le y}$ 是刁藩圖的。 ⊠

4.2 刁藩圖全函數是遞歸函數

定理 **4.4** 刁藩圖全函數對複合、最小化及原始遞運算都是封閉的。

〔證明〕複合：若全函數 $f(y^{(m)}), g_1(x^{(n)}), \cdots, g_m(x^{(n)})$ 都是刁藩圖的，則欲證明函數

$$h(x^{(n)}) = f(g_1(x^{(n)}), \cdots, g_m(x^{(n)}))$$

也是刁藩圖的。這是因為

$$\begin{aligned} & y = h(x^{(n)}) \\ & \Longleftrightarrow \exists t_1, \cdots, t_m [t_1 = g_1(x^{(n)}) \bigwedge \cdots \bigwedge t_m = g_m(x^{(n)}) \bigwedge y = f(t_1, \cdots, t_m)]. \end{aligned}$$

由表示法可知，函數 $h(x^{(n)})$ 是刁藩圖的。

最小化：若刁藩圖全函數 $f(y, x^{(n)})$ 是解析的，則欲證明函數

$$h(x^{(n)}) = \min_y [f(y, x^{(n)}) = 0]$$

也是刁藩圖的。這是因為

$$y = h(x^{(n)}) \Longleftrightarrow (\forall t)_{\le y} [f(y, x^{(n)}) = 0 \bigwedge (t = y \bigvee f(t, x^{(n)}) \neq 0)].$$

由定理 4.3 可知，量詞 $(\forall t)_{\le y}$ 是刁藩圖的，所以函數 $h(x_1, \cdots, x_n)$ 是刁藩圖的。

原始遞歸：若全函數 $f(x^{(n)}), g(x^{(n+2)})$ 是刁藩圖的，且函數 $h(x^{(n+1)})$ 滿足：

$$h(0, x^{(n)}) = f(x^{(n)}),$$

$$h(y+1, x^{(n)}) = g(y, h(y, x^{(n)}), x^{(n)}),$$

則欲證明函數 $h(x^{(n+1)})$ 也是刁藩圖的。由定理 2.4 中遞歸函數 $T(i, w)$ 的性質知：對於

$$h(0, x^{(n)}), \cdots, h(y, x^{(n)}),$$

存在一個整數 $u \in N$ 使得

$$T(i, u) = h(i, x^{(n)}), \ \ i = 0, 1, \cdots, y.$$

因為

$$\begin{aligned} z = h(y, x^{(n)}) \ \Longleftrightarrow \ & \exists\, u (\forall t)_{\le y} \Big[T(0, u) = f(x^{(n)}) \bigwedge \Big(t = y \bigvee \\ & T(t+1, u) = g(t, T(t, u), x^{(n)}) \Big) \bigwedge z = T(y, u) \Big], \end{aligned}$$

所以函數 $h(y, x^{(n)})$ 是刁藩圖的。 ⊠

定理 **4.5** 一個全函數是刁藩圖的其充份必要條件為它是遞歸的。

〔證明〕對任意整數 $k \in N$, 定義函數 $C_k(x) = k$。由定義 2.1 知

$$C_0(x) = N(x) = 0, C_1(x) = C(x) = 1$$

皆為遞歸函數，又

$$C_{k+1}(x) = C_k(x) + C_1(x),$$

所以 $C_k(x) = k$ 也是遞歸函數。已知函數 $x+y, xy$ 是遞歸的。對任意一個非負整數係數多項式

$$P(x_1, \cdots, x_n)$$

而言，它可由遞歸函數 $C_k(x), x+y, xy$ 經有限次複合而成，所以非負整數係數多項式都是遞歸的。

（$\Rightarrow$）先證明：每一個刁藩圖函數都是遞歸的。設函數 $f(x_1, \cdots, x_n)$ 是刁藩圖的，則存在兩個非負整數係數的多項式 P, Q 使得

$$\begin{aligned} y = f(x_1, \cdots, x_n) \quad & \Longleftrightarrow \exists t_1, \cdots, t_m \\ & [P(x_1, \cdots, x_n, y, t_1, \cdots, t_m) = Q(x_1, \cdots, x_n, y, t_1, \cdots, t_m)]. \end{aligned}$$

對任意 $y, t_1, \cdots, t_m$, 由定理 2.4 可知，存在一個 u 使得

$$y = T(0, u), t_i = T(i, u), i = 1, \cdots, m.$$

因此函數 $f(x_1, \cdots, x_n)$ 可表為

$$\begin{aligned} f(x_1, \cdots, x_n) &= y \\ &= T\Big(0, \min_u \Big[P(x_1, \cdots, x_n, T(0,u), \cdots, T(m,u)) \\ &\qquad = Q(x_1, \cdots, x_n, T(0,u), \cdots, T(m,u))\Big]\Big) \\ &= T\Big(0, \min_u \Big[|P(x_1, \cdots, x_n, T(0,u), \cdots, T(m,u)) \\ &\qquad - Q(x_1, \cdots, x_n, T(0,u), \cdots, T(m,u))| = 0\Big]\Big) \end{aligned}$$

因此函數 $f(x_1, \cdots, x_n)$ 是由遞歸函數 $P, Q, T(i,w), |x-y|$ 透過複合及最小化運算所生成的一個遞歸函數。

（$\Leftarrow$）證明：每一個遞歸函數都是刁藩圖的。由初始函數知道：

$$\begin{aligned} C(x) &= 1, \\ S(x) &= x+1, \\ N(x) &= 0, \\ U_i^n(x_1, \cdots, x_n) &= x_i, i = 1, \cdots, n \end{aligned}$$

都是刁藩圖的，由定理 4.4 可知，刁藩圖函數對複合、最小化及原始遞歸運算都是封閉的，所以遞歸函數是刁藩圖的。 ⊠

4.3 希爾伯特第十問題的證明

定理 **4.6** 設 S 是一個刁藩圖集，其餘集 $N-S$ 不是刁藩圖的，則全函數

$$D_S(x)=\begin{cases}0, & x\in S\\ 1, & x\in N-S\end{cases}$$

不是遞歸的。

〔證明〕若全函數 $D_S(x)$ 是遞歸的，則由定理 4.5 可知 $D_S(x)$ 也是刁藩圖的，因此存在一個刁藩圖表現，使得

$$y=D_S(x)\Longleftrightarrow\exists y_1,\cdots,y_m[D(x,y,y_1,\cdots,y_m)=0].$$

由邏輯式子可看出，方程式

$$D(x,1,y_1,\cdots,y_m)=0$$

是集合 $N-S$ 的一個刁藩圖表現，因此集合 $N-S$ 是刁藩圖的。因此全函數 $D_S(x)$ 不是遞歸的。 ⊠

定理 **4.7** 不存在演算法來判定刁藩圖方程式是否有非負整數解。

〔證明〕已知存在一個一維度的刁藩圖集 S，其餘集 $N-S$ 不是刁藩圖的。令方程式

$$D(x,y_1,\cdots,y_n)=0$$

是刁藩圖集 S 的一個刁藩圖表現。若存在演算法來判定刁藩圖方程式是否有非負整數解，則任給 $x\in N$，我們可利用此算法來判定是否 $x\in S$，也就是說，存在演算法來求出下面函數的函數值：

$$D_S(x)=\begin{cases}0, & x\in S,\\ 1, & \in N-S.\end{cases}$$

因此函數 $D_S(x)$ 是可計算的，也就是遞歸的。此結果與定理 4.6 矛盾。因此不存在演算法來判定刁藩圖方程式是否有非負整數解。 ⊠

由定理 4.7 我們可推廣到整數解的結果。

定理 **4.8** 不存在演算法來判定刁藩圖方程式是否有整數解。

〔證明〕任給一個刁藩圖方程式

$$D(x_1,\cdots,x_n)=0, \tag{4.1}$$

由 Lagrange's 定理：每一個非負整數均可表為四個整數的平方和。可得知方程式 (4.1) 存在非負整數解的充份必要條件為刁藩圖方程式：

$$D\Big((x_{1,1}^2+x_{1,2}^2+x_{1,3}^2+x_{1,4}^2),\cdots,(x_{n,1}^2+x_{n,2}^2+x_{n,3}^2+x_{n,4}^2)\Big)=0. \tag{4.2}$$

存在整數解。若存在演算法來判定任意刁藩圖方程式是否有整數解，則存在演算法來判定方程式 (4.2) 是否有整數解，也就是說存在演算法判定方程式 (4.1) 是否有非負整數解。此與定理 4.7 的結果矛盾。因此不存在演算法來判定任意刁藩圖方程式是否有整數解。 ⊠

參 考 書 目

[1] 胡久稔，希爾伯特第十問題，九章出版社。

[2] M. D. Davis, Arithmetical problems and recursively enumerable predicates, *Jounal of Symbolic Logic,* 15(1953), pp. 33-41.

[3] M. D. Davis, *Computability and Unsolvability*, McGraw-Hill, New York, 1958.

[4] M. D. Davis, H. Putnam, and J. Robinson, The decision problem for exponential diophantine equations, *Annals of Mathematics,Second Series,* 74 (1961), pp. 425-436.

[5] M. D. Davis, Hilbert's tenth problem is unsolvable, *the American Mathematical Monthly*, 80 (1973), pp. 233-269.

[6] M. D. Davis, Y. V. Matiyasevich and J. Robinson, Hilbert's tenth problem, diophantine equations: positive aspects of a negative solution, *Proceedings of Symposia in Pure Mathematics*,Vol 28(1976), pp. 323-378.

[7] J. P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens, Diophantine representation of the set of prime numbers, *The American Mathematical Monthly*, 83 (1976), pp. 449-464.

[8] J. P. Jones and Y. V. Matiyasevich, Proof of recursive unsolvability of Hilbert's Tenth Problem, *The American Mathematical Monthly*, 98(1991), pp. 689-709.

[9] J. L. Lagrange, *Nouv. Mem. Acad. Roy. Sc. de Berlin*, 1770, Berlin, 1772, pp. 123-133; Oeuvres, 3, 1869, pp. 189-201. See also the edition of Diophantus published by G. werthein, pp. 324-330.

[10] Y. V. Matiyasevich, Diofantovost' perechislimykh mnozhestv, *Doklady Akademii Nauk SSSR,* 191 (1970), pp. 279-282 (Russian). Improved English translattion: Enumerable sets are Diophatine. *SovietMathematics, Doklady,* 11 (1970), pp. 354-358.

[11] Y. V. Matiyasevich, Diophantine representation of recursively enumerable predicates, *Actes du Congres International des Mathematiciens*, vol. 1 (1970), pp. 235-238, Paris, Gauthier-Villars.

[12] Y. V. Matiyasevich, Some purely mathematical results inspired by mathematical logic. In Robert E. Butts and Jaakko Hintikka, editors, *Logic, Foundations of Mathematics, and Computablity theory*, vol. 1 of *Proceedings of the*

Fifth International Congress of Logic, Mathodology and philosophy of Science, pp. 121-127, London, Ontario, Canada. D. Reidel Publishing Company, Dordrecht, Holland (1977).

[13] Y. V. Matiyasevich and J. Robinson, Reduction of an arbitrary diophantine equation to one in 13 unknowns, *Acta Arithmetica*, 27(1975), pp. 521-553.

[14] Y. V. Matiyasevich, *Hilbert's Tenth Problem*, Nauka Publishers, 1993.

[15] H. Putnam,An unsolvable problem in number theory, *J. Symb. Logic*, 25 (1960), pp. 220-232.

[16] J. Robinson, General Recursive Functions, *Proceedings of the American Mathematical Society*, vol.1 (1950), pp. 703-718.

[17] J. Robinson, Existential definability in arithmetic, *Trans. Amer. Math. Soc.* , 72(1952), pp. 437-449.

[18] J. Robinson,Unsolvable Diophantine problems, *Proceedings of the Amer. Math. Soc.*, 22(1969), pp. 534-538.