4. Groebner 基底

4.1 多項式次序

在談論 Groebner 基底之前，必須先對多項式的次序（order），也就是多項式的單項大小做一些定義，以下就是一些常見到的單項次序定義。

定義 4.1 (Lexicographic order)：令$\alpha=(\alpha_1,\alpha_2,...,\alpha_n)$及$\beta=(\beta_1,\beta_2,...,\beta_n)\in \mathbf{Z}_{\geq 0}^n$，如果在向量差$\alpha-\beta$中最左邊第一個非 0的元素(entry)是正的，則稱$\alpha >_{lex} \beta$，反之則$\alpha <_{lex} \beta$。這種次序定義大小稱為Lexicographic order(簡稱 lex)。我們稱兩單項$x^{\alpha} >_{lex} x^{\beta}$，如果$\alpha >_{lex} \beta$。

例 4.1：

a．令 $\alpha=(2,3,0)$，$\beta=(1,4,2)$，則$\alpha-\beta=(1,-1,-2)$，因為$\alpha-\beta$最左邊第一個非0元素是1，因此$x_1^2x_2^3x_3^0 >_{lex} x_1^1x_2^4x_3^2$。

b．令 $\alpha=(4,1,3)$，$\beta=(4,1,1)$，則$\alpha-\beta=(0,0,2)$，因為$\alpha-\beta$最左邊第一個非0元素是2所以$x_1^4x_2^1x_3^3 >_{lex} x_1^4x_2^1x_3^2$。

定義 4.2 (Graded Lex order)：令$\alpha,\beta\in \mathbf{Z}_{\geq \mathbf{0}}^n$.我們稱$\alpha >_{grlex} \beta$如果$|\alpha|=\sum_{i=1}^{n}\alpha_i > |\beta|=\sum_{i=1}^{n}\beta_i$，或者 $|\alpha|=|\beta|$且$\alpha >_{lex} \beta$。這種次序大小定義稱為Grad Lex order(簡稱Grlex)。

例 4.2：

a．$\alpha=(2,1,3) >_{grlex} \beta=(2,0,3)$，因為$|(2,1,3)|=6>|(2,0,3)|=5$，因此$x_1^2x_2^1x_3^3 >_{grlex} x_1^2x_2^0x_3^3$.

b．$\alpha=(1,3,4) >_{grlex} \beta=(1,2,5)$，因為$|(1,3,4)|=|(1,2,5)|$且$(1,3,4) >_{lex} (1,2,5)$，因此$x_1^1x_2^3x_3^4 >_{grlex} x_1^1x_2^2x_3^5$.

以上所介紹的兩種項次序的定義是比較常用到的定義，當然還有其他的次序定義，如 Graded Reverse Lex order 等，其詳細的定義這邊不再詳述，有興趣之讀者可參閱 Cox, Little and O'Shea (2007)。

任何一個多項式都是由幾個單項式所構成的，可藉由所選取的項次序來排列出各單項的大小順序。以下我們將介紹幾個名詞定義。

定義 4.3：令 $f=\sum_{\alpha} a_{\alpha}\mathbf{x}_{\alpha} \in k[x_1,x_2,...,x_n]$，是一個非0的多項式，而且令> 是一個項次序(term– ordering)。

(1) f 的聯合度(multidegree)為

$$\text{multideg}(f)=\max\left(\alpha \in \mathbf{Z}_{\geq \mathbf{0}}^{n} \mid a_{\alpha} \neq 0\right)$$

這裡的 max 是根據所選取的項次序決定的。

(2) f 的領導係數(leading coefficient)為

$$\text{LC}(f)=a_{\text{multideg}(f)} \in k$$

(3) f 的領導單項(leading monomial)為

$$\text{LM}(f)=\mathbf{x}^{\text{multideg}(f)}$$

(4) f 的領導項(leading term)為

$$\text{LT}(f)=\text{LC}(f)\cdot\text{LM}(f)$$

例 4.3：令 $f=6x_1x_2x_3-4x_1x_2^2+7x_2x_3^3-x_1^2x_3^2-2x_1^4-x_2^3$，令 $>_{lex}$ 為lex order，則

$$\text{multideg}(f)=(4,0,0)$$

$$\text{LC}(f)=-2$$

$$\text{LM}(f)=x_1^4$$

$$\text{LT}(f)=-2x_1^4.$$

在這裡我們已經可以很清楚的瞭解一個多項式的領導項是如何被定義的。每一個

多項式都有一個領導項，則可利用領導項定義出一個理想的 Groebner 基底。

4.2 Groebner 基底

定義 4.4：令$\boldsymbol{I} \subset k[x_1, x_2, ..., x_n]$為一非0的理想，則：

(i) 我們以LT($\boldsymbol{I}$)表示為理想$\boldsymbol{I}$中多項式的領導項所形成的集合。因此

$$\mathrm{LT}(\boldsymbol{I}) = \{cx^{\alpha} : \text{存在} f \in \boldsymbol{I}, \text{使得} \mathrm{LT}(f) = cx^{\alpha}\}$$

(ii) 我們以$\langle \mathrm{LT}(\boldsymbol{I}) \rangle$表示為集合LT($\boldsymbol{I}$)中的元素所生成的理想。

定義 4.5：設$\boldsymbol{I}$是一個理想，固定一個項次序，若有一組多項式$g_1, g_2, ..., g_s$使得

$$\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), ..., \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(\boldsymbol{I}) \rangle$$

則這組多項式$\{g_1, g_2, ..., g_s\}$稱為Groebner基底。

例 4.4（續3.1）：理想$\boldsymbol{I}(\overline{E})$的基底為$\left\{x_1^2 - 1, x_2^2 - 1, \frac{3}{4} + \frac{1}{4}x_1 + \frac{1}{4}x_2 - \frac{1}{4}x_1x_2\right\}$，項次序為lex order，其Groebner基底則為

$$\left\{x_1^2 - 1,\ x_2^2 - 1,\ \frac{3}{4} + \frac{1}{4}x_1 + \frac{1}{4}x_2 - \frac{1}{4}x_1x_2,\ x_1 + 1, x_2 + 1\right\}。$$

假如一個有限集合$G = \{g_1, g_2, ..., g_s\}$為理想$\boldsymbol{I}$的Groebner基底，則理想$\boldsymbol{I}$可由$g_1, g_2, ..., g_s$所生成，也就是說$\boldsymbol{I} = \langle g_1, g_2, ..., g_s \rangle$。但是當$\boldsymbol{I} = \langle f_1, f_2, ..., f_m \rangle$時，$\langle \mathrm{LT}(f_1), \mathrm{LT}(f_1), ..., \mathrm{LT}(f_1) \rangle$與$\langle \mathrm{LT}(\boldsymbol{I}) \rangle$可能是不同的兩個理想，而根據定義可知$\mathrm{LT}(f_i) \in \mathrm{LT}(\boldsymbol{I}) \subset \langle \mathrm{LT}(\boldsymbol{I}) \rangle$，這也暗示著$\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), ..., \mathrm{LT}(f_m) \rangle \subset \langle \mathrm{LT}(\boldsymbol{I}) \rangle$，因此理想$\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), ..., \mathrm{LT}(f_m) \rangle$一定被包含於理想$\langle \mathrm{LT}(\boldsymbol{I}) \rangle$之中，但不代表兩者會相等。

一個理想的 Groebner 基底是如何找出來的呢？其實 Groebner 基底的求法，就是多元多次除法推廣的運用，因此我們首先來介紹的是多元多次的除法定理。

定理 4.1 (除法定理, Cox, Little and O'Shea (2007), Section2.3)：令$F=\{f_1, f_2,..., f_s\}$，$f_1, f_2,..., f_s \in k[x_1, x_2,..., x_n]$是一個多元多次多項式組，$f \in k[x_1, x_2,..., x_n]$是另一個多元多次多項式，則 f 可以表示為

$$f = a_1 f_1 + a_2 f_2 + ... + a_s f_s + r$$

其中的$a_i, r \in k[x_1, x_2,..., x_n]$，且 $r=0$ 或 r 的任何一項都不能被 LT(f_1), LT(f_2),..., LT(f_s)中任何一個所整除，此時我們稱 r 為在 F 上 f 的餘式(remainder)。

假使 $a_i f_i \neq 0$，則

$$\text{multideg}(f) \geq \text{multideg}(a_i f_i)$$

由除法定理所得到的 r 並不會唯一，我們以下舉個例子就可看出這個事實。

例 4.5：令 $f_1 = x_1 x_2 + 1$， $f_2 = x_2^2 - 1 \in k[x_1, x_2]$，使用 lex order，$f = x_1 x_2^2 - x_1$被 $F=(f_1, f_2)$(按前後順序)來除的話，則

$$f = x_2 \cdot f_1 + 0 \cdot f_2 + (-x_1 - x_2)$$

如果現在換成 f 被 $F=(f_2, f_1)$來除的話，則

$$f = x_1 \cdot f_2 + 0 \cdot f_1 + 0$$

由例 4.5 這個例子看出，當除式的順序不一樣時，可能得到的餘式 r 可能就是不同的結果，因此，當餘式 $r=0$ 時，可說 $f \in \langle f_1, f_2 \rangle$，但是當 $r \neq 0$，並不代表 $f \notin \langle f_1, f_2 \rangle$，$r=0$ 對於理想裡的元素並不是一個必要條件。但是除式如果是一個 Groebner 基底，不論除式裡面的元素先後順序，餘式 r 會是唯一的。

定理 4.2 (Cox, Little and O'Shea (2007), Section 2.6)：設 $\boldsymbol{I}$ 為一個理想，令 $G=\{g_1, g_2,..., g_t\}$是理想 $\boldsymbol{I}$ 的 Groebner 基底，對任何$f \in k[x_1, x_2,..., x_n]$， f 被 G 除所得到的餘式會是唯一的，即存在唯一的$r \in k[x_1, x_2,..., x_n]$，滿足下面兩個性質：

(1) r 中的任何一項都不能被 LT(g_1), LT(g_2),..., LT(g_t)中任何一個整除。

(2) 存在一 $g \in \boldsymbol{I}$，使得 $f = g + r$。

特別當 $f \in \boldsymbol{I}$，若且唯若餘式 $r=0$

接下來我們將為餘式 r 做一些符號上的定義。

定義 4.6：$f_1, f_2, ..., f_t \in k[x_1, x_2, ..., x_n]$，令 $F = (f_1, f_2, ..., f_t)$。若 $f \in k[x_1, x_2, ..., x_n]$，我們用 $\overline{f}^F$ 來表示多項式 f 被 F 除所得到的餘式。

定義 4.7：設 $f, g \in k[x_1, x_2, ..., x_n]$為兩非0的多項式，而且 $\mathbf{x}^r$ 為 LM(f)與 LM(g)的最低公倍式(least common multiple)，則 S - 多項式定義為

$$S(f,g) = \frac{\mathbf{x}^r}{\mathrm{LT}(f)} \cdot f - \frac{\mathbf{x}^r}{\mathrm{LT}(g)} \cdot g \qquad (4.2)$$

這個運算將會把 f 與 g 兩多項式的領導項消掉。

我們可以推得以下的這個定理：

定理 4.3 (Cox, Little and OShea (2007), Section 2.6)：設 $\boldsymbol{I}$ 是一個理想，而 $G = \{g_1, g_2, ..., g_t\}$是理想 $\boldsymbol{I}$ 的Groebner基底，若且唯若$\overline{S(g_i, g_j)}^G = 0$ (G裡的元素為某種排列方式)，$\forall i \neq j$。

由定理 4.3 知，Groebner 基底中的多項式都會被 G 所整除；而當任何 S -多項式被一組基底除了以後餘式不等於 0，則把餘式加進來當作是此基底的另一個多項式元素，使得原來的基底多了一個元素，一直重複做(4.2)式 S-多項式的運算，最後直到不管怎麼除，餘式都是 0 的時候，此時，我們便可以得到了這組多項式所生成的理想的 Groebner 基底，這種算 Groebner 基底的演算法稱為 Buchberger's A1gorithm。

例 4.6：多項式次序用grlex order，設 $f_1 = x_1^3 - 2x_1x_2$ ， $f_2 = x_1^2x_2 - 2x_2^2 + x_1$ ，理想$\mathbf{I} = \langle f_1, f_2 \rangle$，$G = \{f_1, f_2\}$是理想 $\boldsymbol{I}$ 的基底但不是Groebner基底，因為

$$S(f_1, f_2) = \frac{x_1^3x_2}{x_1^3} \cdot (x_1^3 - 2x_1x_2) - \frac{x_1^3x_2}{x_1^2x_2} \cdot (x_1^2x_2 - 2x_2^2 + x_1) = -x_1^2$$

根據除法定理知$\overline{S(f_1, f_2)}^G = -x_1^2 \neq 0$。此時令 $f_3 = -x_1^2$，把 f_3 加進去G中，因此 $G = \{f_1, f_2, f_3\}$。此時的$\overline{S(f_1, f_2)}^G = 0$，而

$$S(f_1, f_3) = \frac{x_1^3}{x_1^3} \cdot \left(x_1^3 - 2x_1x_2\right) - \frac{x_1^3}{x_1^2} \cdot \left(-x_1^2\right) = -2x_1x_2 \text{ 。}$$

根據除法定理知，$\overline{S(f_1, f_3)}^{G} = -2x_1x_2 \neq 0$，此時令 $f_4 = -2x_1x_2$，加入 f_4 到G，這時候集合 $G = \{f_1, f_2, f_3, f_4\}$。這時候，同樣做(4.2)式$S$-多項式的運算，故可得到$\overline{S(f_1, f_2)}^{G} = \overline{S(f_1, f_3)}^{G} = 0$，再對 f_1與 f_4這兩元素做S-多項式運算，即可得到 $S(f_1, f_4) = -2x_1x_2^2 = x_2 \cdot f_4$，因此 $\overline{S(f_1, f_4)}^{G} = 0$。但是 $S(f_2, f_3) = -2x_2^2 + x_1$，所以餘式 $\overline{S(f_2, f_3)}^{G} = -2x_2^2 + x_1 \neq 0$，此時令 $f_5 = -2x_2^2 + x_1$，把 f_5 加入G，得到 $G = \{f_1, f_2, f_3, f_4, f_5\}$，最後，$\overline{S(f_i, f_j)}^{G} = 0$，$\forall 1 \leq i < j \leq 5$ 。因此，在次序為grlex order之下，理想 $\boldsymbol{I}$ 的Groebner基底為$\{f_1, f_2, f_3, f_4, f_5\}$，即

$$\{f_1, f_2, f_3, f_4, f_5\} = \left\{x_1^3 - 2x_1x_2, x_1^2x_2 - 2x_2^2 + x_1, -x_1^2, -2x_1x_2, -2x_2^2 + x_1\right\}\text{。}$$

在相同項次序下計算出的 Groebner 基底可能不相同，也就是說 Groebner 基底並不唯一，因此後人另外定義 reduced Groebner 基底，在 reduced Groebner 基底的限制條件下，可證明出理想 $\boldsymbol{I}$ 在相同次序有唯一一組的 reduced Groebner 基底，但在此不再詳述其定義。根據Buchberger's A1gorithm，算出一個理想 $\boldsymbol{I}$ 的Groebner基底的方法還蠻繁雜的，因此市面上有一些數學軟體都有計算 Groebner 基底的功能，如：Maple、Mathematica、COCOA 等，都可幫助計算 Groebner 基底。在求多元多次方程組的解的時候，可利用求出其 Groebner 基底，因為我們知道這多元多次方程組與 Groebner 基底有相同的解集合，則可利用求 Groebner 基底的解，就可找出原來方程組的解是多少。在下一章節，我們將利用 Groebner 基底找出實驗設計中相異試驗點的個數。