多项式模上全次数除法

冯玉瑜 * 王旭明 邓建松 †
(中国科技大学数学系)

摘要 本文首先介绍了利用 Gröbner 基求解 Syzygy 模生成元的方法, 在对方法做出进一步分析的基础上, 给出了一元模上的多项式辗转相除法, 这种除法相对于已有的方法有许多优点.

关键词 计算代数几何, Gröbner 基, Syzygy 模, 全次数除法
中图法分类号 O187.1
AMS Classification(1991) 14Q10, 68U07

§1 引言

Gröbner 基方法首先是由 Buchberger([5]) 在 1965 年提出, 从七十年代中期开始, 该方法被进一步地完善、推广. 到今天, 它已成为计算代数几何中的一个核心工具. 无论是在理论研究中, 还是在实际应用中, 都有其用武之地. Gröbner 基方法可以应用于各种能被转化为与理想或子模有关的实际问题的解决中, 例如, 多元多项式方程组求解, 几何定理机器证明, 多元多项式齐次方程组合冲 (Syzygy) 生成元求解, 参数曲面的隐式化等, 甚至在三色问题, 整数规划 ([1]) 中都有其应用. Gröbner 基理论发展至今, 已有大量文献可供查阅, 如 [5, 6, 7, 8, 9] 等文章或专著 [1, 2].

但是在实际应用 Gröbner 基时, 也有很多的缺陷, 其难以预见的高计算复杂度, 使我们在应用 Gröbner 基方法时, 总要仔细考虑有没有其它的方法. 本文给出的就是在特定情形中, 可以不必严格按照 Buchberger 算法, 求出子模的生成元, 也可以得到类似于 Gröbner 基所满足的良好性质.

根据我们的计算经验, 这种除法是相当有用的, 在 [10] 一文中, 我们探讨了利用全次数除法, 求解几何连续性中跨边界导数自由度的问题。

我们首先在第 2 节中列举了利用 Gröbner 基方法求解 Syzygy 的已有结果. 另外, 根据实际计算的经验, 我们在第 3 节中提出了一元多项式模中元素的辗转相除法, 经过处理后的子模生成元, 具有很好的性质: 即在构造子模中元素时, 不会出现 (全) 首项相消的情形. 虽然选择某种项序 (在一元时项序只有一种, 即 $1 < x < x^2 < \cdots$) 时, 模上的 Gröbner 基可以

*973 项目 "数学机械化"(No. G1998030600)、国家自然科学基金与教委博士点基金资助
†中国科大校内青年基金资助

满足这种条件，但这里所给方法可以使得有些情形下不必把生成元化为 Gröbner 基，也可以使生成元具有与 Gröbner 基相类似的某种特征.

§2 Syzygy 与 Gröbner 基方法

§2.1 Syzygy 的定义

为了简单起见，把无限域 k 上 n 变量多项式环 $k[x_1, x_2, \ldots, x_n]$ 记为 A. $I = \langle f_1, \ldots, f_s \rangle$ 为 A 的一个理想. 考虑 $A-$ 模同态 $\phi: A^s \longrightarrow I$, 其定义为

$$(h_1, \ldots, h_s) \mapsto \sum_{i=1}^{s} h_i f_i.$$

则有 A 模同构： $I \cong A^s/\ker(\phi)$.

定义 2.1 映射 ϕ 的核 (Kernel) 称为 $1 \times s$ 阶矩阵 $[f_1, \ldots, f_s]$ 的 Syzygy 模，用 Syz $(f_1, \ldots, f_s)$ 表示. Syz $(f_1, \ldots, f_s)$ 的一个元素 $(h_1, \ldots, h_s)$ 称为 $[f_1, \ldots, f_s]$ 的一个 Syzygy, 它满足方程 $h_1 f_1 + \cdots + h_s f_s = 0$.

由上面定义可见， Syz $(f_1, \ldots, f_s)$ 就是系数为多项式的如下线性方程的解：

$$f_1 \chi_1 + \cdots + f_s \chi_s = 0, \tag{2.1}$$

其中方程的解 χ_i 也是 A 中的多项式.

注意，映射 ϕ 也可以看作矩阵乘法：

$$\phi(h_1, \ldots, h_s) = [f_1, \ldots, f_s][h_1, \ldots, h_s]^{\mathrm{T}} = \sum_{i=1}^{s} h_i f_i.$$

也就是说，如果 F 为 $1 \times s$ 矩阵 $[f_1, \ldots, f_2]$, 而 $\boldsymbol{h} = [h_1, \ldots, h_s]^{\mathrm{T}} \in A^s$, 那么 $\phi(h_1, \ldots, h_s) = F\boldsymbol{h}$, Syz $(f_1, \ldots, f_s)$ 就是线性方程组 $F\boldsymbol{h} = 0$ 的所有解 $\boldsymbol{h}$. 利用这种矩阵乘法的观点，很容易就把 Syzygy 的概念推广到多个方程的情形.

下面给出一个 Syzygy 的例子. 设 $A = \mathbb{Q}[x, y, z, w]$ ，而

$$I = \langle x^2 - yw, xy - wz, y^2 - xz \rangle。$$

映射 $\phi: A^3 \longrightarrow I$ 的定义如下：

$$(h_1, h_2, h_3) \mapsto h_1(x^2 - yw) + h_2(xy - wz) + h_3(y^2 - xz)。$$

那么 $(y, -x, w)$ 和 $(-z, y, -x)$ 都是 $[x^2 - yw, xy - wz, y^2 - xz]$ 的 Syzygy 。

类似于 (2.1) 这样的系数为 A 中多项式的齐次方程，或者更一般地，系数为 A^m 中元素的齐次方程，在环论与模论中扮演着非常重要的角色. 而且 Syzygy 模在 Gröbner 基理论中也处于举足轻重的地位；特别地，应用它可以改进计算 Gröbner 基的 Buchberger 算法 ([1, 2]).

§2.2 Syzygy 模生成元的求解

由于 Syz $(f_1,\ldots,f_s)$ 为 A^s 的子模，因此它是有限生成的. 我们现在的目标就是给出计算 Syz $(f_1,\ldots,f_s)$ 生成元的方法. 在下面的定理中都首先假设已固定了 A 上的一个项序.

定理 2.1 ([1]) 设 $G=\{g_1,g_2,\ldots,g_t\}$ 是某一理想的 Gröbner 基，而且 g_i 都是首一多项式. 对所有的 $1\leqslant i<j\leqslant t$, $k_1^{(i,j)},\ldots,k_t^{(i,j)}$ 是 g_i 和 g_j 的 S 多项式 $S(g_i,g_j)$ 被 G 简化为零多项式过程中产生的系数（利用多元多项式的 Euclid 除法可得到这些系数），即

$$S(g_i,g_j)=\sum_{\ell=1}^{t}k_\ell^{(i,j)}g_\ell.$$

令

$$s_{ij}=\frac{X_{ij}}{X_i}\boldsymbol{e}_i-\frac{X_{ij}}{X_j}\boldsymbol{e}_j-(h_1^{(i,j)},\ldots,h_t^{(i,j)})\in A^t,$$

其中 $X_i=\mathrm{lm}\,(g_i),X_j=\mathrm{lm}\,(g_j),X_{ij}=\mathrm{lcm}\,(X_i,X_j)$，而 $\boldsymbol{e}_i,\boldsymbol{e}_j$ 为 A^t 的自由基. 则集合 $\{s_{ij}|1\leqslant i<j\leqslant t\}$ 是 Syz $(g_1,\ldots,g_t)$ 的一个生成集.

定理 2.2 ([1]) 设 $F=\{f_1,\ldots,f_m\}$ 为 A 中非零多项式集合，其不一定构成某一理想的 Gröbner 基，而 $G=\{g_1,\ldots,g_t\}$ 是 F 生成理想的 Gröbner 基，而且仍设 g_i 为首一多项式. 则由 Gröbner 基的计算方法，可知有 $t\times m$ 阶矩阵 M 和 $m\times t$ 阶矩阵 T 使得

$$[f_1,\ldots,f_m]=[g_1,\ldots,g_t]M,\quad [g_1,\ldots,g_t]=[f_1,\ldots,f_m]T.$$

利用定理 2.1 可以计算出 Syz $(g_1,\ldots,g_t)$ 的生成元 $\{s_1,\ldots,s_r\}$. 记矩阵 I_m-TM 的列向量为 $r_1,\ldots,r_m$, 则

$$\mathrm{Syz}\,(f_1,\ldots,f_m)=\langle Ts_1,\ldots,Ts_r,r_1,\ldots,r_m\rangle\subset A^m.$$

特别地，我们有如下推论：

推论 当所考虑的多项式为单变量时，则方程

$$f_1h_1+\cdots+f_mh_m=0$$

的解集（即 Syzygy 模）只由矩阵 I_m-TM 的列向量生成，这里的 T,M 定义同定理 2.2, 只是它们分别是 $m\times 1$ 阶和 $1\times m$ 阶的.

证明 由于所考虑的多项式为一元的, 所以对给定的 $f_1,\cdots,f_m$, 其所生成理想的 Gröbner 基就是这些多项式的最大公约式 $g=\gcd(f_1,\cdots,f_m)$ 。即只有一个多项式。所以此时矩阵 M 和 T 的阶数分别是 $1\times m$ 和 $m\times 1$ 。其元素的构造，不必用 Buchberger 算法，实际上由一元多项式的 Euclid 除法就可得到。

而方程 $gh=0$ 的解集显然为 $\{0\}$ ，所以由定理 2.2 ，

$$\mathrm{Syz}\,(f_1,\cdots,f_m)=\langle r_1,\cdots,r_m\rangle,$$

其中 $r_1,\cdots,r_m$ 为矩阵 I_m-TM 的列向量。 ■

我们下面就是用这个推论来进行讨论的。

§3 一元多项式模上的辗转相除法

众所周知，在有理数域或实数域上的一元多项式环中， Euclid 除法是一个相当重要的工具，如果利用它辗转进行多项式除法，可以得出两个多项式的最大公约式．而且计算 Gröbner 基的 Buchberger 算法从某种角度上来，实际上也就是辗转相除法在多个变量时的推广．在本节我们一律用 A 来表示 $\mathbb{R}[x]$ 或 $\mathbb{Q}[x]$.

我们知道在模中也有 Buchberger 算法，但由于我们现在考虑的一元多项式模，因此没有必要像通用的 Buchberger 算法那样进行化简给定子模的生成元．因为要运用该算法，首先要选定项序是 TOP 或 POT, 而这两种选法，都在位置上有一定的偏颇．比如说 A^3 有两个元素为

$$\boldsymbol{f}_1 = \begin{bmatrix} x^2+x+1 \\ x-1 \\ 3x-1 \end{bmatrix}, \qquad \boldsymbol{f}_2 = \begin{bmatrix} x^2+2x+3 \\ x^2+x-1 \\ 2x^2+3x \end{bmatrix}. \tag{3.1}$$

选取项序为 POT, 且位置顺序为 $1>2>3$, 则

$$\mathrm{lt}\,(\boldsymbol{f}_1) = x^2\boldsymbol{e}_1, \qquad \mathrm{lt}\,(\boldsymbol{f}_2) = x^2\boldsymbol{e}_1,$$

因此可以进行 Buchberger 算法中的一个循环，但实际上虽然化简了第一个分量（降低了其次数），但也同时升高了后两个分量的次数．导致这种现象的本质原因就在于这里项序的选取不可避免地要厚此薄彼．当给定子模的生成元时，我们希望构造一组新的生成元，使得子模中任一元素相对于生成元的组合中不会出现全首项相消的情形．因此我们下面给出新的算法：即一元模中两个元素的辗转相除法．我们首先考虑生成元只有两个元素时的情形．

§3.1 定义和元素的标准表示

给定 A^m 中的一个元素 $\boldsymbol{f}$, 其所有分量多项式的最高次数 n 称为 $\boldsymbol{f}$ 的 **全次数**, 记为 $\mathrm{Deg}\,(\boldsymbol{f}) = n$. 记 $\boldsymbol{f} = [f_1, \ldots, f_m]^T$, 而且设

$$f_i = a_n^{(i)}x^n + a_{n-1}^{(i)}x^{n-1} + \cdots + a_0^{(i)}, \quad i = 1, 2, \ldots, m,$$

若 f_i 次数 n_i 小于 n, 则令 $a_{n_0}^{(i)}, \ldots, a_n^{(i)}$ 全为 0. 但我们知道至少有一个多项式的首项系数不为 0. 这样我们可以把 $\boldsymbol{f}$ 写为如下的标准形式：

$$\boldsymbol{f} = \begin{bmatrix} a_n^{(1)} \\ \vdots \\ a_n^{(m)} \end{bmatrix} x^n + \begin{bmatrix} a_{n-1}^{(1)} \\ \vdots \\ a_{n-1}^{(m)} \end{bmatrix} x^{n-1} + \cdots + \begin{bmatrix} a_0^{(1)} \\ \vdots \\ a_0^{(m)} \end{bmatrix}, \tag{3.2}$$

其中 $[a_n^{(1)}, \ldots, a_n^{(m)}]^T x^n$ 称为 $\boldsymbol{f}$ 的 **全首项**, 记为 $\mathrm{LM}\,(\boldsymbol{f})$; 而向量 $[a_n^{(1)}, \ldots, a_n^{(m)}]^T$ 称为 $\boldsymbol{f}$ 的 **全首项向量**, 记为 $\mathrm{LV}\,(\boldsymbol{f})$. 由全首项的定义显然有如下关系式：

$$\mathrm{LM}\,(k\boldsymbol{f}) = \mathrm{lm}\,(k)\mathrm{LM}\,(\boldsymbol{f}), \tag{3.3}$$

其中 $k \in A$.

§3.2 两个元素的辗转相除法

定义 3.2 给定 A^m 中两个元素 $\boldsymbol{f}_1, \boldsymbol{f}_2$, $\mathrm{Deg}\,(\boldsymbol{f}_i) = n_i, i = 1, 2$. 若其全首项向量对应分量成比例，比例常数为 k, 即 $\mathrm{LV}\,(\boldsymbol{f}_1) = k\mathrm{LV}\,(\boldsymbol{f}_2)$, 而且 $n_1 \geqslant n_2$, 则称 $\boldsymbol{f}_1$ 可被 $\boldsymbol{f}_2$ 进行 **一步除法**；这时 $kx^{n_1-n_2}$ 为 **商**, $\boldsymbol{f}_1 - kx^{n_1-n_2}\boldsymbol{f}_2$ 为 **余元** 或 **余式**；若 $n_1 < n_2$, 则称 $\boldsymbol{f}_2$ 可被 $\boldsymbol{f}_1$ 进行 **一步除法**, 而 $\frac{1}{k}x^{n_2-n_1}$ 为 **商**, $\boldsymbol{f}_2 - \frac{1}{k}x^{n_2-n_1}\boldsymbol{f}_1$ 为 **余元** 或 **余式**. 若不能进行一步除法，则称 $\boldsymbol{f}_1$ 和 $\boldsymbol{f}_2$ 相对于一步除法是 **简化的**.

例如, (3.1) 中的两个元素就不可以进行一步除法, 即它们是相对于一步除法是简化的, 而如下两个元素却可以进行一步除法：

$$\boldsymbol{f}_1 = \begin{bmatrix} x+1 \\ 2x-1 \\ -1 \end{bmatrix}, \qquad \boldsymbol{f}_2 = \begin{bmatrix} x^2+2x+3 \\ 2x^2+x-1 \\ 2x+3 \end{bmatrix}.$$

由一步除法的定义，显然有如下定理：

定理 3.3 给定两个可以进行一步除法的 A^m 中的元素 $\boldsymbol{f}_1, \boldsymbol{f}_2$, 其生成的模也就是除式与余式生成的模.

设 $\boldsymbol{f}_1, \boldsymbol{f}_2$ 为两个可进行一步除法的元素，且余元非零，用 $\boldsymbol{f}_1^{[1]}$ 和 $\boldsymbol{f}_2^{[2]}$ 表示经过运算后所得的余元与除式，其生成的子模与 $\langle \boldsymbol{f}_1, \boldsymbol{f}_2 \rangle$ 相同. 而两个新元素生成元的全次数都不会超过 $\max(n_1, n_2)$. 实际上若 $n_1 \neq n_2$, 则两个新元素的全次数严格小于 $\max(n_1, n_2)$. 用 $\{\boldsymbol{f}_1, \boldsymbol{f}_2\} \hookrightarrow \{\boldsymbol{f}_1^{[1]}, \boldsymbol{f}_2^{[1]}\}$ 表示该运算过程；若新得到的这两个元素又可以进行一步除法，则再进行一次运算，得到的余式（非零）和除法中的除式记作 $\boldsymbol{f}_1^{[2]}$ 和 $\boldsymbol{f}_2^{[2]}$, 则仍然有 $\langle \boldsymbol{f}_1, \boldsymbol{f}_2 \rangle = \langle \boldsymbol{f}_1^{[2]}, \boldsymbol{f}_2^{[2]} \rangle$, 对这两个新元素我们还可以考虑一步除法的可行性. 如此辗转应用该运算，直到余式为零，或者最后得到两个不可再进行一步除法的元素 $\boldsymbol{g}_1, \boldsymbol{g}_2$. 在这两种情况下，都必有最终元素生成的子模与最初给定的子模相同. 即如当所得为两个不可再进行一步除法的元素时，有 $\langle \boldsymbol{f}_1, \boldsymbol{f}_2 \rangle = \langle \boldsymbol{g}_1, \boldsymbol{g}_2 \rangle$, 我们用记号 $\{\boldsymbol{f}_1, \boldsymbol{f}_2\} \hookrightarrow_* \{\boldsymbol{g}\}$ 或 $\{\boldsymbol{f}_1, \boldsymbol{f}_2\} \hookrightarrow_* \{\boldsymbol{g}_1, \boldsymbol{g}_2\}$ 表示重复运算过程. 称这里由可以进行一步除法的 $\boldsymbol{f}_1, \boldsymbol{f}_2$ 开始，经过多次一步除法，得到一个元素 $\boldsymbol{g}$ 或者是两个相对于一步除法简化的 $\boldsymbol{g}_1$ 和 $\boldsymbol{g}_2$ 的过程，就为一元多项式模上的 **辗转相除法**, 或者称为 **简化过程**. 上述运算过程实际上说明了如下定理：

定理 3.4 任何由两个元素生成的子模，必存在两个新生成元，这两个元素相对于一步除法是简化的，或者生成元只是一个元素.

定理 3.5 给定两个相对于一步除法是简化的元素 $\boldsymbol{g}_1, \boldsymbol{g}_2$, $k_1, k_2 \in A$ 为任意多项式， $\boldsymbol{g} = k_1\boldsymbol{g}_1 + k_2\boldsymbol{g}_2$, 即 $\boldsymbol{g} \in \langle \boldsymbol{g}_1, \boldsymbol{g}_2 \rangle$, 则有

$$\mathrm{Deg}\,(\boldsymbol{g}) = \max(\mathrm{Deg}\,(k_1\boldsymbol{g}_1), \mathrm{Deg}\,(k_2\boldsymbol{g}_2)).$$

证明 考虑 $\boldsymbol{g} = k_1\boldsymbol{g}_1 + k_2\boldsymbol{g}_2$ 两边的全首项,

1. 若 $\mathrm{Deg}\ (k_1\boldsymbol{g}_1) \neq \mathrm{Deg}\ (k_2\boldsymbol{g}_2)$, 则 $\mathrm{LM}\ (\boldsymbol{g})$ 即为这两者全次数较大者的全首项，从而

$$\mathrm{Deg}\ (\boldsymbol{g}) = \max(\mathrm{Deg}\ (k_1\boldsymbol{g}_1), \mathrm{Deg}\ (k_2\boldsymbol{g}_2)),$$

即结论成立.

2. 若 $\mathrm{Deg}\ (k_1\boldsymbol{g}_1) = \mathrm{Deg}\ (k_2\boldsymbol{g}_2)$, 而此时却有

$$\mathrm{Deg}\ (\boldsymbol{g}) < \max(\mathrm{Deg}\ (k_1\boldsymbol{g}_1), \mathrm{Deg}\ (k_2\boldsymbol{g}_2))$$

成立，则必有

$$\mathrm{LM}\ (k_1\boldsymbol{g}_1) + \mathrm{LM}\ (k_2\boldsymbol{g}_2) = 0,$$

从而有

$$\mathrm{LV}\ (\boldsymbol{g}_1) = \frac{\mathrm{lc}\ (k_2)}{\mathrm{lc}\ (k_1)}\mathrm{LV}\ (\boldsymbol{g}_2),$$

这即 $\boldsymbol{g}_1$ 与 $\boldsymbol{g}_2$ 相对于一步除法不是简化的. 导致矛盾，也就是说此时仍只能有

$$\mathrm{Deg}\ (\boldsymbol{g}) = \max(\mathrm{Deg}\ (k_1\boldsymbol{g}_1), \mathrm{Deg}\ (k_2\boldsymbol{g}_2))$$

成立.

综合这两种情形可知定理成立.

这个定理说明的是, 当我们已知一个子模的两个相对于一步除法是简化的生成元时, 当用这两个元素构造子模中元素时, 不会出现全首项相消的情形. 这就非常类似多项式环上的由 Gröbner 基构造理想中元素时的情形.

§3.3 多个元素的辗转相除法

当所处理的子模不只由两个元素生成时, 我们可以把前面的一步除法进行如下推广. 因为所谓两个向量对应分量成比例，即指这两个向量是线性相关的. 因此我们有如下定义：

定义 3.3 给定 A^m 中的 k 个元素 $\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_k$, 其全次数分别为 $n_1, n_2, \ldots, n_k$. 若其全首项向量是线性相关的，则称这 k 个元素可进行 **一步除法**；而且由于 k 个向量线性相关，则存在 k 个常数 $c_1, c_2, \ldots, c_k$ 使得

$$\sum_{\ell=1}^{k} c_\ell \mathrm{LV}\ (\boldsymbol{f}_\ell) = 0,$$

设 $c_{k_0}\boldsymbol{f}_{k_0} = \max_\ell(\mathrm{Deg}\ (c_\ell \mathrm{LM}\ (\boldsymbol{f}_\ell))$ (显然 $c_{k_0} \neq 0$), 记

$$\boldsymbol{g} := \boldsymbol{f}_{k_0} + \frac{1}{c_{k_0}} \sum_{\substack{\ell=1 \\ \ell \neq k_0}} c_\ell x^{d-n_\ell} \boldsymbol{f}_\ell$$

若 $\boldsymbol{g} = 0$, 则记 $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_k, \boldsymbol{g}\} \backslash \{\boldsymbol{f}_{k_0}\}$ 为经上述一步除法后的 **余元（式）集合**；否则若 $\boldsymbol{g} \neq 0$, 则称 $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_k, \boldsymbol{g}\} \backslash \{\boldsymbol{f}_{k_0}\}$ 为经上述一步除法后的 **余元（式）集合**. 显然 $\mathrm{Deg}\ (\boldsymbol{g}) < \mathrm{Deg}\ (\boldsymbol{f}_{k_0})$.

同两个生成元时类似，一旦给定一个子模的 k 个生成元 $\boldsymbol{f}_1,\ldots,\boldsymbol{f}_k$，若能进行一步除法，我们记经一步除法后的元素为 $\boldsymbol{f}_1^{[1]},\ldots,\boldsymbol{f}_{k_1}^{[1]}$，并用记号 $\{\boldsymbol{f}_1,\ldots,\boldsymbol{f}_k\}\hookrightarrow\{\boldsymbol{f}_1^{[1]},\ldots,\boldsymbol{f}_{k_1}^{[1]}\}$ 表示这个过程. 这里 $k_1=k$ 或 $k-1$.

同样对新得的 k_1 个元素又可以考虑一步除法的可行性，并在可以进行时，计算出新的余元集合. 如此进行下去，直到有 $t(t\leqslant k)$ 个元素 $\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t$，其不能再进行一步除法，或者 $t=1$. 另一方面由于所考虑元素在 A^m 中，因此最后显然有 $t\leqslant\min(k,m)$. 用记号表示上述除法过程为 $\{\boldsymbol{f}_1,\ldots,\boldsymbol{f}_k\}\hookrightarrow_*\{\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t\}$，我们把上述过程称为多个元素的 **辗转相除法**.

定义 3.4 若 $\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t$ 为 A^m 中非零元素，其全首项向量是相关无关的，则称这 t 个元素相对于一步除法是 **简化的**. 特别地，若 $t=1$，则我们规定 $\boldsymbol{g}=0$ 相对于一步除法是简化的.

同样我们有如下两个定理：

定理 3.6 设 $\boldsymbol{f}_1,\ldots,\boldsymbol{f}_k$ 为给定的 A^m 中元素，$\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t$ 为其经辗转相除法所得的结果，即相对于一步除法是简化的，则有

$$\langle\boldsymbol{f}_1,\ldots,\boldsymbol{f}_k\rangle=\langle\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t\rangle. \tag{3.4}$$

这个定理说明了任何子模都有一个相对于一步除法是简化的生成元.

定理 3.7 若 A^m 中元素 $\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t$ 相对于一步除法是简化的，$\boldsymbol{g}\in\langle\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t\rangle$，即存在 $\alpha_1,\ldots,\alpha_t\in A$，使得

$$\boldsymbol{g}=\sum_{\ell=1}^{t}\alpha_\ell\boldsymbol{g}_\ell,$$

则 $\mathrm{Deg}\,(\boldsymbol{f})=\max\limits_{1\leqslant\ell\leqslant t}\mathrm{Deg}\,(\alpha_\ell\boldsymbol{g}_\ell)$.

证明 考虑 $\boldsymbol{g}=\alpha_1\boldsymbol{g}_1+\cdots+\alpha_t\boldsymbol{g}_t$ 两边的全首项，

1. 在 $\alpha_\ell\boldsymbol{g}_\ell$ 中，若次数等于 $\max\limits_{1\leqslant\ell\leqslant t}(\mathrm{Deg}\,(\alpha_\ell\boldsymbol{g}_\ell))$ 的项只有一个，则显然有

$$\mathrm{Deg}\,(\boldsymbol{g})=\max_{1\leqslant\ell\leqslant t}(\mathrm{Deg}\,(\alpha_\ell\boldsymbol{g}_\ell)),$$

即结论成立.

2. 否则，设 $\alpha_{\ell_1}\boldsymbol{g}_{\ell_1},\ldots,\alpha_{\ell_r}\boldsymbol{g}_{\ell_r}$ 项的次数等于 $\max\limits_{1\leqslant\ell\leqslant t}(\mathrm{Deg}\,(\alpha_\ell\boldsymbol{g}_\ell))$，若此时有

$$\mathrm{Deg}\,(\boldsymbol{g})<\max_{1\leqslant\ell\leqslant t}(\mathrm{Deg}\,(\alpha_\ell\boldsymbol{g}_\ell)),$$

则

$$\mathrm{LV}\left(\sum_{i=1}^{r}\alpha_{\ell_i}\boldsymbol{g}_{\ell_i}\right)=0,$$

即

$$\sum_{i=1}^{r}\mathrm{lc}\,(\alpha_{\ell_i})\mathrm{LV}\,(\boldsymbol{g}_{\ell_i})=0,$$

这与已知 $\boldsymbol{g}_1,\ldots,\boldsymbol{g}_t$ 相对于一步除法是简化的矛盾. 所以结论仍然成立.

综合这两种情形可知定理成立.

这两个定理说明：当我们已知一个子模的生成元，通过辗转相除法，可以获得其相对于一步除法是简化的新生成元. 对这新的生成元而言，要构造子模中元素时，不会出现全首项相消的情形. 这就非常类似多项式环上的由 Gröbner 基构造理想中元素时的情形. 关于这一点我们在 [10] 中研究几何连续性跨边界导数取值时要用到.

参考文献

[1] W. W. Adams and P. Loustaunau, An introduction to Gröbner bases, Graduate Studies in Math., Vol.3, American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning, Gröbner bases, A computational approach to commutative algebra, Graduate Texts in Math., Vol.141, Springer-Verlag, 1993.

[3] —, Gröbner basis methods for multivariate splines, Mathematical Methods in Computer Aided Geometric Design, T. Lyche and L. L. Schumaker(eds.), Academic Press, New York, 1989, 92-104.

[4] L. J. Billera and L. L. Rose, A dimension series for multivariate splines, Discrete Comput. Geom., 6(1991), 107-128.

[5] B. Buchberger, An algorithmic criterion for the solvability of algebraic systems of equations, Aequationes Math., 4(1970), 374-383.

[6] —, A theoretical basis for the reduction of polynomials to canonical form, ACM SIGSAM Bull. 39(1976), 19-29.

[7] —, Gröbner bases: an algorithmic method in polynomial ideal theory, in Multidimensional Systems Theory, N. K. Bose(ed.), D. Reidel Publishing Company, Dordrecht-Boston-Lancaser, 1985, 184-232.

[8] —, History and basic features of the critical pair completion procedure, J. Symb. Comp., 3(1987), 3-38.

[9] D. A. Cox, Introduction to Gröbner bases, in Applications of Computational Algebraic Geometry, American Mathematical Society Short Course, D. A. Cox and B. Sturmfels eds., 1–24, 1997.

[10] 冯玉瑜，陈长松，邓建松，多项式模上的全次数除法在 CAGD 中的应用，已投稿.

The Total Degree Division in Polynomial Module

Feng Yuyu Wang Xuming Deng Jiansong

(*Dept. of Mathematics of USTC*)

Abstract At first, we list the known results about solving Syzygy using Gröbner basis. From these, we propose a division algorithm between elements in module of single-variant polynomials, which is an extension of classical Euclid division algorithm in polynomial ring. There are some good attributes upon some exist methods.

Key words computational algebraic geometry, Gröbner basis, syzygy module, total degree division