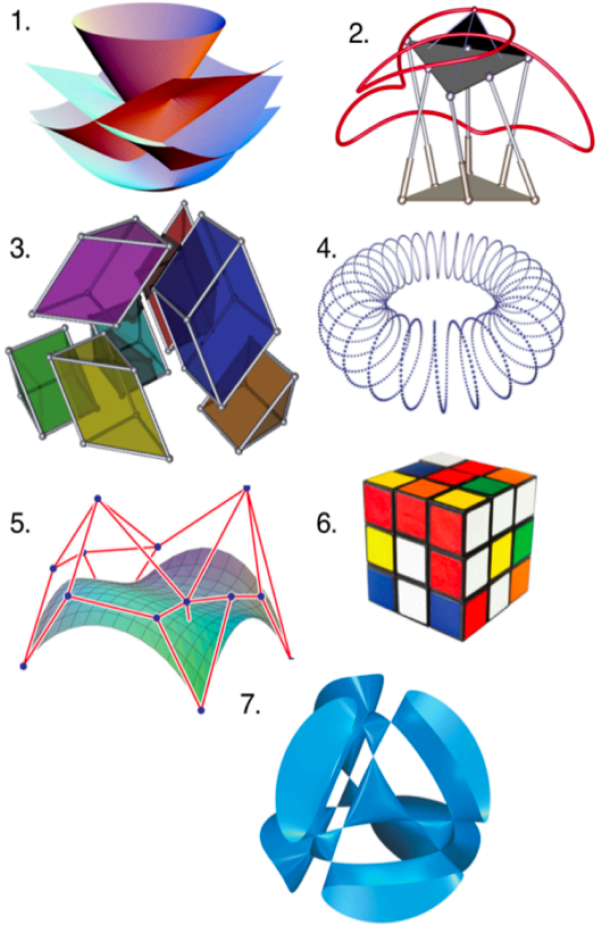
计算机代数

牟晨琪

北航沙河校区E403-7
chenqi.mou@buaa.edu.cn

2020年春



第二章

多项式消元与方程求解

多项式代数概述

多项式代数

是研究多项式和多项式系统所定义或导出的代数与几何对象的结构、性质、特征、表示、相互关系及计算的代数学.

- 非线性: 最简单
- 多项式方程组的求解：主要研究问题之一
- 构造性：VS 传统交换代数与代数几何
- 算法：正确性与终止性

解多项式方程组

Example

$\mathbb{Q}[x_1, \ldots, x_n]$ 中的多项式方程组 (循环 n 根系统)

$$\begin{cases} x_1 + x_2 + \cdots + x_n = 0, \\ x_1x_2 + x_2x_3 + \cdots + x_nx_1 = 0, \\ \quad\cdots\cdots \\ x_1x_2\cdots x_n - 1 = 0. \end{cases}$$

- $n = 8$: >2 小时 (VS 线性方程组)

而 $\tilde{\mathcal{K}}$ 为 $\mathcal{K}$ 的扩域: 多项式方程组求解就是求由 $\mathcal{F} \subseteq \mathcal{K}[\boldsymbol{x}]$ 所定义的方程组 $\mathcal{F} = 0$ 在 $\tilde{\mathcal{K}}$ 中的解并将其适当地表示出来.

1. $\mathcal{F} = 0$ 在 $\tilde{\mathcal{K}}$ 中是否有解? 有解的话解的个数有限还是无限?
2. 如何表示 $\mathcal{F} = 0$ 在 $\tilde{\mathcal{K}}$ 中的解?
3. 如何求出 $\mathcal{F} = 0$ 在 $\tilde{\mathcal{K}}$ 中的所有解?

多项式消元

- Gröbner 基/三角列：高斯消去法的推广

Example

$\mathbb{Q}[x_1, \ldots, x_n]$ 中的多项式方程组 (循环 n 根系统)

$$\begin{cases} x_1 + x_2 + \cdots + x_n = 0, \\ x_1x_2 + x_2x_3 + \cdots + x_nx_1 = 0, \\ \quad\cdots\cdots \\ x_1x_2\cdots x_n - 1 = 0. \end{cases}$$

三角分解: $n = 3$

$$\begin{aligned} \mathcal{T}_1 &= [x_1 - 1, {x_2}^2 + x_2 + 1, x_3 + x_2 + 1], \\ \mathcal{T}_2 &= [x_1^2 + x_1 + 1, x_2 - 1, x_3 + x_1 + 1], \\ \mathcal{T}_3 &= [x_1^2 + x_1 + 1, x_2 + x_1 + 1, x_3 - 1]. \end{aligned}$$

Gröbner 基

奥地利计算机科学家B. Buchberger

Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. Ph.D. thesis, Universitat Innsbruck, Austria (1965) (An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal)

- W. Gröbner 是他的导师

多项式理想成员判定问题

生成理想

给定多项式 $F_1, \ldots, F_r \in \mathcal{K}[\boldsymbol{x}]$, 则由 $F_1, \ldots, F_r$ 生成的理想为

$$\langle F_1, \ldots, F_r \rangle := \{G_1 F_1 + \cdots + G_r F_r : \ G_i \in \mathcal{K}[\boldsymbol{x}], i = 1, \ldots, r\}.$$

理想成员判定问题

给定 $\mathcal{K}[\boldsymbol{x}]$ 中的多项式 G 和理想 $\mathfrak{a}$, 判断 G 是否属于 $\mathfrak{a}$.

- 判断 G 是否属于 $\langle F_1, \ldots, F_r \rangle$

- 关于多项式理想的基础问题
- VS 线性空间成员判定问题: $v \in b_1, \ldots, b_s$ 生成的线性空间?

多项式：从项的角度, 项序

变元 $x_1, \ldots, x_n$ 的所有项组成的集合记为 $\mathfrak{T}(\boldsymbol{x})$: $x_1 < \cdots < x_n$

集合 $\mathfrak{T}(\boldsymbol{x})$ 上的全序关系 $<$ 称为项序 (term ordering), 如果:

1. 对任意 $\mu_1, \mu_2, \mu \in \mathfrak{T}(\boldsymbol{x})$, 若 $\mu_1 < \mu_2$, 则 $\mu\mu_1 < \mu\mu_2$;
2. $<$ 为良序, 即 $\mathfrak{T}(\boldsymbol{x})$ 中任意非空子集关于 $<$ 都有最小元.

设 $F = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$ 为 $\mathcal{R}[\boldsymbol{x}]$ 中的非零多项式, $<$ 为 $\mathcal{R}[\boldsymbol{x}]$ 上的项序, 则 F 关于 $<$ 的

- 首项 (head term): $\mathrm{ht}_<(F) := \max_<\{\mu : \mu \in \mathfrak{T}(F)\}$
- 首项系数 (head coefficient): $\mathrm{hc}_<(F) := \mathrm{coef}(F, \mathrm{ht}_<(F))$
- 首单项式 (head monomial): $\mathrm{hm}_<(F) := \mathrm{hc}_<(F) \cdot \mathrm{ht}_<(F)$

在不引起混淆的情况下, 分别简写为 $\mathrm{ht}(F)$, $\mathrm{hc}(F)$ 和 $\mathrm{hm}(F)$.

多项式约化

多项式约化

给定项序 $<$, 对任意 $F, P \in \mathcal{K}[\boldsymbol{x}]$, 若存在项 $\mu \in \mathfrak{T}(F)$ 与 $\nu \in \mathfrak{T}(\boldsymbol{x})$ 使得 $\mu = \nu \cdot \mathrm{ht}(P)$, 则称 F 模 P 可约化 (reducible). 令

$$G = F - \frac{\mathrm{coef}(F, \mu)}{\mathrm{hc}(P)} \cdot \nu P,$$

称 F 模 P 消去 μ 约化 (reduce) 至 G, 记作 $F \xrightarrow[\mu]{P} G$ ($F \xrightarrow{P} G$).

设 $\mathcal{P} \subseteq \mathcal{K}[\boldsymbol{x}]$, 若存在多项式 $P \in \mathcal{P}$ 使得 $F \xrightarrow{P} G$, 则称 F 模 $\mathcal{P}$ 约化至 G, 记作 $F \xrightarrow{\mathcal{P}} G$. 这时也称 F 模 $\mathcal{P}$ 可约化; 否则称 F 模 $\mathcal{P}$ 已约化 (reduced).

$$F \xrightarrow{\mathcal{P}} F_1 \xrightarrow{\mathcal{P}} \cdots \xrightarrow{\mathcal{P}} F_{m-1} \xrightarrow{\mathcal{P}} R,$$

且 R 模 $\mathcal{P}$ 已约化, 则称 R 为 F 模 $\mathcal{P}$ 的范式 (normal form). 称由 F 求得 R 的过程为 F 模 $\mathcal{P}$ 的约化 (reduction), 记作 $F \xrightarrow[*]{\mathcal{P}} R$

多项式约化

- 多项式 F 模多项式组 $\{P_1, \ldots, P_r\}$ 的范式是 R 意味着什么？
  $\Longrightarrow F - R \in \langle P_1, \ldots, P_r \rangle$

Example

对多项式环 $\mathcal{K}[x, y]$, 取变元序为 $x < y$, 项序为字典序. 考虑多项式 $F = x^2y^3 + 2\,xy^2 + x + 1$ 与多项式集合 $\mathcal{P} = \{P_1, P_2\}$, 其中 $P_1 = y^2, P_2 = xy + 1$. F 模 $\mathcal{P}$ 的两种约化过程如下所示:

$$F \xrightarrow[x^2y^3]{P_1} 2\,xy^2 + x + 1 \xrightarrow[xy^2]{P_2} x - 2\,y + 1,$$

$$F \xrightarrow[x^2y^3]{P_2} xy^2 + x + 1 \xrightarrow[xy^2]{P_1} x + 1.$$

由项序诱导的多项式序

多项式序

$\mathcal{K}[\boldsymbol{x}]$ 上的任意项序 $<$ 都可以诱导多项式序 (polynomial ordering) $<'$ 如下:

1. 对任意非零多项式 $F \in \mathcal{K}[\boldsymbol{x}]$, $0 <' F$;
2. 对任意非零多项式 $F, G \in \mathcal{K}[\boldsymbol{x}]$, $F <' G$ 当且仅当

$$\mathrm{ht}(F) < \mathrm{ht}(G) \quad \text{或} \quad \mathrm{ht}(F) = \mathrm{ht}(G) \text{ 且 } F\text{−hm}(F) <' G\text{−hm}(G).$$

为简单起见, 我们将 $<$ 诱导的多项式序 $<'$ 仍记为 $<$.

- 比较项的大小 $\Longrightarrow$ 比较多项式的大小：多项式序是良序
- 多项式约化后在上述多项式序的意义下变大变小?

多项式约化

算法 14 多项式约化 $([Q_1,\ldots,Q_s],R) := \mathsf{PolyRed}([P_1,\ldots,P_s],F)$

输入: $[P_1,\ldots,P_s] \subseteq \mathcal{K}[\boldsymbol{x}], F \in \mathcal{K}[\boldsymbol{x}]$.

输出: $[Q_1,\ldots,Q_s] \subseteq \mathcal{K}[\boldsymbol{x}], R \in \mathcal{K}[\boldsymbol{x}]$ 满足

(a) $F = \sum_{i=1}^{s} Q_i P_i + R$;

(b) R 模 $\{P_1,\ldots,P_s\}$ 已约化;

(c) 当 $Q_i P_i \neq 0$ 时, $\mathrm{ht}(Q_i P_i) \leqslant \mathrm{ht}(F)$.

$Q_i := 0\ (i = 1,\ldots,s), R := F$;

while R 模 $\{P_1,\ldots,P_s\}$ 可约化 **do**

选取 P_i 使得 R 模 P_i 可约化;

选取单项式 λ 使得 $R \xrightarrow{P_i} R - \lambda P_i$;

$R := R - \lambda P_i$;

$Q_i := Q_i + \lambda$;

end

return $([Q_1,\ldots,Q_s], R)$;

- 终止性

多项式理想成员判定问题

Example

$$F \xrightarrow[x^2y^3]{P_1} 2\,xy^2 + x + 1 \xrightarrow[xy^2]{P_2} x - 2\,y + 1,$$

$$F \xrightarrow[x^2y^3]{P_2} xy^2 + x + 1 \xrightarrow[xy^2]{P_1} x + 1.$$

- 多项式约化的过程并不唯一, 所得范式也不唯一.
- $R=0$ 是判定理想成员问题的充分条件, 但不是必要条件.

Example

令 $\mathcal{Q} = \{Q_1 = xy + 1, Q_2 = y^2 - 1\}$, 有

$$xy^2 - x \xrightarrow[xy^2]{Q_1} -y - x;$$

$$xy^2 - x \xrightarrow[xy^2]{Q_2} 0.$$

多项式理想的有限生成性

项理想

设 $S \subseteq \mathbb{N}^n$, 称 $\mathcal{K}[\boldsymbol{x}]$ 中由项集 $\{\boldsymbol{x}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in S\}$ 生成的理想为项理想 (term ideal), 记作 $\langle \boldsymbol{x}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in S \rangle$.

- 项理想中的元素并非都是项.

引理 (证明)

设项理想 $\mathfrak{a} = \langle \boldsymbol{x}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in S \rangle$, 则项 $\boldsymbol{x}^{\boldsymbol{\beta}} \in \mathfrak{a}$ 当且仅当存在 $\boldsymbol{\alpha} \in S$ 使得 $\boldsymbol{x}^{\boldsymbol{\alpha}} \mid \boldsymbol{x}^{\boldsymbol{\beta}}$.

命题 (证明)

设 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为项理想, $F \in \mathcal{K}[\boldsymbol{x}]$ 为任意多项式, 则下列命题等价

1. $F \in \mathfrak{a}$;
2. F 的每一项都在 $\mathfrak{a}$ 中;
3. F 是 $\mathfrak{a}$ 中项的 $\mathcal{K}$ 线性组合.

多项式理想的有限生成性

Dickson 引理 (证明)

对于 $\mathcal{K}[\boldsymbol{x}]$ 中的任意项理想 $\mathfrak{a} = \langle \boldsymbol{x}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in S \rangle$，均存在 $\boldsymbol{\alpha}(1), \ldots, \boldsymbol{\alpha}(s) \in S$ 使得 $\mathfrak{a} = \langle \boldsymbol{x}^{\boldsymbol{\alpha}(1)}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}(s)} \rangle$.

- 对变元个数 n 用归纳法：假设 $n-1$ 时成立

$$\mathfrak{b} = \langle \boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}} : \exists\ l \in \mathbb{N} \text{ 使得 } \boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}} y^l \in \mathfrak{a} \rangle \subseteq \mathcal{K}[\boldsymbol{x}_{n-1}].$$

- 有限生成，分而治之

$$\begin{array}{ccc}
\boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}(1)} y^m, & \ldots & , \boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}(s)} y^m, \\
\boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}_0(1)}, & \ldots & , \boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}_0(s_0)}, \\
\boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}_1(1)} y, & \ldots & , \boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}_1(s_1)} y, \\
 & \ldots & \\
\boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}_{m-1}(1)} y^{m-1}, & \ldots & , \boldsymbol{x}^{\tilde{\boldsymbol{\alpha}}_{m-1}(s_{m-1})} y^{m-1}
\end{array}$$

Hilbert 基定理

设 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为非零理想, 而 $\mathrm{ht}(\mathfrak{a})$ 为 $\mathfrak{a}$ 中元素的首项构成的集合, 即 $\mathrm{ht}(\mathfrak{a}) := \{\mathrm{ht}(F) : F \in \mathfrak{a}\}$

练习 (简单说明)

设 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为理想, 则下列结论成立:

1. $\langle \mathrm{ht}(\mathfrak{a}) \rangle$ 是项理想;
2. 存在 $G_1, \ldots, G_s \in \mathfrak{a}$ 使得 $\langle \mathrm{ht}(\mathfrak{a}) \rangle = \langle \mathrm{ht}(G_1), \ldots, \mathrm{ht}(G_s) \rangle$.

Hilbert 基定理 (证明)

多项式环 $\mathcal{K}[\boldsymbol{x}]$ 中理想均存在有限生成元. 即对任意 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$, 存在 $G_1, \ldots, G_s \in \mathfrak{a}$ 使得 $\mathfrak{a} = \langle G_1, \ldots, G_s \rangle$.

Hilbert 基定理

D. Hilbert

P. Gordan

A famous quote attributed to Gordan about David Hilbert's proof of Hilbert's basis theorem, a result which vastly generalized his result on invariants, is "This is not mathematics; this is theology."

Hilbert 基定理的等价条件

Hilbert 基定理

多项式环 $\mathcal{K}[\boldsymbol{x}]$ 中理想均存在有限生成元. 即对任意 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$, 存在 $G_1, \ldots, G_s \in \mathfrak{a}$ 使得 $\mathfrak{a} = \langle G_1, \ldots, G_s \rangle$.

理想的升链条件 (证明)

对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意理想升链 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$, 均存在 $N \geqslant 1$ 使得 $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \mathfrak{a}_{N+2} = \cdots$.

等价性 (不证明)

对多项式环 $\mathcal{K}[\boldsymbol{x}]$, 下列条件等价.

1. (升链条件) 对 $\mathcal{K}[\boldsymbol{x}]$ 中的任意理想升链 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$, 均存在 $N \geqslant 1$ 使得 $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \mathfrak{a}_{N+2} = \cdots$.
2. (最大元条件) $\mathcal{K}[\boldsymbol{x}]$ 中的任意非空理想集族均有最大元.
3. (有限基条件) $\mathcal{K}[\boldsymbol{x}]$ 中的任意理想均有有限基.

Gröbner 基：定义和存在性

定义

给定 $\mathcal{K}[\boldsymbol{x}]$ 上的项序, $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为理想. 设 $\mathfrak{a}$ 的有限子集 $\mathcal{G} = \{G_1, \ldots, G_s\}$ 满足

$$\langle \mathrm{ht}(G_1), \ldots, \mathrm{ht}(G_s) \rangle = \langle \mathrm{ht}(\mathfrak{a}) \rangle,$$

则称 $\mathcal{G}$ 为 $\mathfrak{a}$ 的 Gröbner 基 (Gröbner basis).

- 当 $\mathcal{G}$ 为 $\langle \mathcal{G} \rangle$ 的 Gröbner 基时, 也简称 $\mathcal{G}$ 为 Gröbner 基.

存在性

给定项序, 则 $\mathcal{K}[\boldsymbol{x}]$ 中任意理想 $\mathfrak{a}$ 均有 Gröbner 基. 更进一步地, 理想 $\mathfrak{a}$ 的 Gröbner 基也是其有限生成元.

Gröbner 基：性质

Gröbner 基的等价定义 (由定义易得)

给定 $\mathcal{K}[\boldsymbol{x}]$ 上的项序, 理想 $\mathfrak{a}$ 中的集合 $\{G_1, \ldots, G_s\}$ 是 $\mathfrak{a}$ 的 Gröbner 基当且仅当对任意 $F \in \mathfrak{a}$, 存在 G_i 使得 $\mathrm{ht}(G_i) \mid \mathrm{ht}(F)$.

范式计算的惟一性 (证明: 反证)

设 $F \in \mathcal{K}[\boldsymbol{x}]$, 而 $\mathcal{G} = \{G_1, \ldots, G_s\}$ 为 Gröbner 基, 则 F 模 $\mathcal{G}$ 的范式唯一.

- 将 F 模 Gröbner 基 $\mathcal{G}$ 的唯一范式记为 $\mathrm{nform}(F, \mathcal{G})$

理想成员的判定问题 (证明)

设 $F \in \mathcal{K}[\boldsymbol{x}]$, 而 $\mathcal{G} = \{G_1, \ldots, G_s\}$ 为理想 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$ 的 Gröbner 基, 则 $F \in \mathfrak{a}$ 当且仅当 $\mathrm{nform}(F, \mathcal{G}) = 0$.

Gröbner 基：消元性质

取 $\mathcal{K}[\boldsymbol{x}]$ 上的变元序为 $x_1 < \cdots < x_n$, 项序为字典序. 对 $1 \leqslant l \leqslant n$, 记 $\boldsymbol{x}_l = (x_1, \ldots, x_l)$. 对理想 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$, 易证 $\mathfrak{a} \cap \mathcal{K}[\boldsymbol{x}_l]$为 $\mathcal{K}[\boldsymbol{x}_l]$ 中的理想. 称其为 $\mathfrak{a}$ 的第 l 个消去理想 (elimination ideal), 记作 $\mathfrak{a}_l$.

消元定理 (证明)

取 $\mathcal{K}[\boldsymbol{x}]$ 上的变元序为 $x_1 < \cdots < x_n$, 项序为字典序. 设理想 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$, 而 $\mathcal{G}$ 为 $\mathfrak{a}$ 的 Gröbner 基, 则对于任意 l $(0 \leqslant l \leqslant n)$, 集合 $\mathcal{G}_l := \mathcal{G} \cap \mathcal{K}[\boldsymbol{x}_l]$ 为理想 $\mathfrak{a}_l$ 的 Gröbner 基.

示例

取 $\mathbb{C}[x, y, z]$ 上的变元序为 $x < y < z$, 项序为字典序. 此时理想 $\mathfrak{a} = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$ 的 Gröbner 基为

$$[G_1 := x^2y^4 + x^4y^2 - x^2y^2 + 1, \quad G_2 := z + xy^3 + x^3y - xy].$$

由消元定理知, $\mathfrak{a}_1 = \mathfrak{a} \cap \mathbb{C}[x] = \{0\}, \mathfrak{a}_2 = \mathfrak{a} \cap \mathbb{C}[x, y] = \langle G_1 \rangle$.

曲面的隐式化

曲面的隐式化问题

任给有理曲面 (参数方程)

$$S(s,t)=\left(\frac{F(s,t)}{W(s,t)},\frac{G(s,t)}{W(s,t)},\frac{H(s,t)}{W(s,t)}\right), \tag{1}$$

其中 $F, G, H, W \in \mathbb{R}[s,t]$, 并且 $\gcd(F, G, H, W) = 1$, 求不可约多项式 $P \in \mathbb{R}[x,y,z]$, 使得

$$P\left(\frac{F(s,t)}{W(s,t)},\frac{G(s,t)}{W(s,t)},\frac{H(s,t)}{W(s,t)}\right)=0.$$

曲面的隐式化

定理

令 $A = F(s,t) - W(s,t)x$, $B = G(s,t) - W(s,t)y$, $C = H(s,t) - W(s,t)z$, 则有理曲面 (1) 的隐式方程为

$$P(x,y,z) = 0, \quad P \in \langle A, B, C, wW - 1\rangle \cap \mathbb{R}[x,y,z].$$

Example

考虑有理曲面 S:

$$x = \frac{st^2 - t}{st^2}, y = \frac{st + s}{st^2}, z = \frac{2\,s - 2\,t}{st^2}.$$

令 $A = st^2x - (st^2 - t)$, $B = st^2y - (st + s)$, $C = st^2z - (2\,s - 2\,t)$. 计算 $\langle A, B, C, wst^2 - 1\rangle$ 由变元序 $z < x < y < s < t < w$ 确定的字典序 Gröbner 基, 即可得曲面 S 的隐式方程

$$z^2 - 4\,zx - 4\,zy + 4\,x^2 + 8\,xy + 4\,y^2 + 2\,z - 4\,x - 8\,y = 0.$$

Gröbner 基的计算

对于项 $\mu = x_1^{k_1} \cdots x_n^{k_n}$ 和 $\nu = x_1^{l_1} \cdots x_n^{l_n}$, 易证 μ 与 ν 的最小公倍式 $\operatorname{lcm}(\mu, \nu) = x_1^{m_1} \cdots x_n^{m_n}$, 其中 $m_i = \max(k_i, l_i)$.

定义

设 $F, G \in \mathcal{K}[\boldsymbol{x}]$ 为非零多项式, 而 $\mu = \operatorname{lcm}(\operatorname{ht}(F), \operatorname{ht}(G))$, 称

$$\mathrm{S}(F, G) = \operatorname{hc}(G) \cdot \frac{\mu}{\operatorname{ht}(F)} \cdot F - \operatorname{hc}(F) \cdot \frac{\mu}{\operatorname{ht}(G)} \cdot G$$

为 F 和 G 的 S 多项式 (S-polynomial)

Example

取 $\mathbb{R}[x, y]$ 上的变元序为 $x < y$, 项序为字典序, 则多项式 $F = 2\,x^4 y - x^2 y + 2\,x$ 与 $G = 4\,x^3 y^2 + y$ 的 S 多项式为

$$\begin{aligned} \mathrm{S}(F, G) &= 4 \cdot \frac{x^4 y^2}{x^4 y} \cdot (2\,x^4 y - x^2 y + 2\,) - 2 \cdot \frac{x^4 y^2}{x^3 y^2} \cdot (4\,x^3 y^2 + y) \\ &= -4\,x^2 y^2 + 6\,xy. \end{aligned}$$

Gröbner 基的计算

引理

给定 $\mathcal{K}[\boldsymbol{x}]$ 上的项序 $<$. 设多项式集合 $\{G_1, \ldots, G_s\} \subseteq \mathcal{K}[\boldsymbol{x}]$ 满足 $\mathrm{ht}(G_i) = \boldsymbol{x}^{\boldsymbol{\delta}}$ $(1 \leqslant i \leqslant s)$. 又设 $F = \sum_{i=1}^{s} c_i G_i$, 其中 $c_i \in \mathcal{K}$. 若 $\mathrm{ht}(F) < \boldsymbol{x}^{\boldsymbol{\delta}}$, 则 F 可以写作 S 多项式 $\mathrm{S}(G_j, G_k)$ $(1 \leqslant j, k \leqslant s)$ 的 $\mathcal{K}$ 线性组合, 且对任意 j 和 k, $\mathrm{ht}(\mathrm{S}(G_j, G_k)) < \boldsymbol{x}^{\boldsymbol{\delta}}$.

定理: S 对准则 (不证明)

设 $\mathcal{G} = \{G_1, \ldots, G_s\}$ 为理想 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$ 的生成元, 则 $\mathcal{G}$ 是 $\mathfrak{a}$ 的 Gröbner 基当且仅当对任意 $i \neq j$, $\mathrm{S}(G_i, G_j)$ 模 $\mathcal{G}$ 的范式均为 0.

- S 对准则是 Gröbner 基理论的重要结果
- 判定多项式组是否为 Gröbner 基

Gröbner 基的计算

Buchberger 算法

算法 15 Buchberger 算法 $\mathcal{G} := \mathsf{GröbnerBasis}(\mathcal{F})$

输入: $\mathcal{F} = [F_1, \ldots, F_s] \subseteq \mathcal{K}[\boldsymbol{x}]$.
输出: $\mathcal{F}$ 的 Gröbner 基 $\mathcal{G}$, 满足 $\mathcal{F} \subseteq \mathcal{G}$.

$\mathcal{G} := \mathcal{F}$;
$\mathcal{L} := \{\{G_i, G_j\} : G_i, G_j \in \mathcal{G}$ 使得 $G_i \neq G_j\}$;
while $\mathcal{L} \neq \emptyset$ **do**
  $\{G_i, G_j\} := \mathsf{pop}(\mathcal{L})$;
  $R := \mathrm{S}(G_i, G_j)$ 模 $\mathcal{G}$ 的一个范式;
  if $R \neq 0$ **then**
    $\mathcal{L} := \mathcal{L} \cup \{\{G, R\} : G \in \mathcal{G}\}$;
    $\mathcal{G} := \mathcal{G} \cup \{R\}$;
  end
end
return 根据多项式序重排的 $\mathcal{G}$;

- 计算 Gröbner 基的经典算法
- 正确性：$\mathcal{F} \subset \mathcal{G} \subset \langle \mathcal{F} \rangle$, S 对准则
- 终止性：理想的升链条件

第二次大作业

1. 设项序为字典序, 编写程序实现多元多项式 $F \in \mathcal{K}[\boldsymbol{x}]$ 模多元多项式组 $\mathcal{P} \subset \mathcal{K}[\boldsymbol{x}]$ 的约化算法 (书中算法 14 一部分)
2. 设项序为字典序，编写程序实现计算多元多项式组 $\mathcal{F} \subset \mathcal{K}[\boldsymbol{x}]$ 的 Gröbner 基的 Buchberger 算法 (书中算法 15)
3. 利用字典序 Groebner 基进行下述有理曲面的隐式化 (参考本幻灯片的第 23 页)：

$$x = \frac{st^2 - t}{st^2}, y = \frac{st + s}{st^2}, z = \frac{2\,s - 2\,t}{st^2}.$$

格式与时间要求

- 上交作业为电子版，需包含源程序和简单的解决方式描述（例如主要步骤及其计算结果等），后者鼓励用 Latex 写.
- 截止时间为 4 月 10 日，请将作业打包.zip文件以“计算机代数 2–姓名–学号”命名，以同样名称为邮件名发送至 zjwang@buaa.edu.cn.

几点提示

1. 建议用 Maple 软件写，因为已经有常见的有关 Gröbner 基计算的函数
2. 利用 Maple 软件完成作业时的提示
   - Maple 中的 term 和 monomial 的定义跟我们的相反
   - Groebner 软件包: 调用方式 "with(Groebner)"，包含 Gröbner 基计算的常用函数
   - plex(z, y, x): 变元序为 $x < y < z$ 的字典序
   - LeadingTerm(P, plex(z, y, x)): 返回字典序下多项式 P 的首项系数和首项
   - SPolynomial(F, G, plex(z, y, x)): 返回多项式 F 和 G 在字典序下的 S 多项式
   - 可以利用IsBasis(Pset, plex(z, y, x)) 来验证多项式组 Pset 是否为 Gröbner 基, 从而验证第 2 问的程序是否编写正确
   - 利用第 2 问编写的 Buchberger 算法计算第 3 问中所涉及的 Gröbner 基时应该有约 100 次约化
3. 源程序需包含适量的注释

Gröbner 基的计算

Buchberger 算法

算法 15 Buchberger 算法 $\mathcal{G} := \mathsf{GröbnerBasis}(\mathcal{F})$

输入: $\mathcal{F} = [F_1, \ldots, F_s] \subseteq \mathcal{K}[\boldsymbol{x}]$.
输出: $\mathcal{F}$ 的 Gröbner 基 $\mathcal{G}$, 满足 $\mathcal{F} \subseteq \mathcal{G}$.

$\mathcal{G} := \mathcal{F}$;
$\mathcal{L} := \{\{G_i, G_j\} : G_i, G_j \in \mathcal{G}$ 使得 $G_i \neq G_j\}$;
while $\mathcal{L} \neq \emptyset$ **do**
  $\{G_i, G_j\} := \mathsf{pop}(\mathcal{L})$;
  $R := \mathrm{S}(G_i, G_j)$ 模 $\mathcal{G}$ 的一个范式;
  if $R \neq 0$ **then**
    $\mathcal{L} := \mathcal{L} \cup \{\{G, R\} : G \in \mathcal{G}\}$;
    $\mathcal{G} := \mathcal{G} \cup \{R\}$;
  end
end
return 根据多项式序重排的 $\mathcal{G}$;

- 理想成员的判定问题可以算法化解决: $F \in \langle P_1, \ldots, P_r \rangle$?
- 那如何判断两个理想相等呢? $\langle P_1, \ldots, P_r \rangle = \langle Q_1, \ldots, Q_r \rangle$?

约化 Gröbner 基: 验证 $\mathfrak{a} = \mathfrak{b}$?

引理 (显然)

设 $\mathcal{G}$ 为 Gröbner 基, 若 $G \in \mathcal{G}$ 使得 $\mathrm{ht}(G) \in \langle \mathrm{ht}(\mathcal{G} \setminus \{G\}) \rangle$, 则 $\mathcal{G} \setminus \{G\}$ 也是 Gröbner 基.

反复利用上述引理可得到满足如下条件的 Gröbner 基 $\mathcal{G}'$:

1. $\mathcal{G}'$ 中多项式均首一;
2. 对任意 $G \in \mathcal{G}'$, $\mathrm{ht}(G) \notin \langle \mathrm{ht}(\mathcal{G}' \setminus \{G\}) \rangle$.

称为理想 $\mathfrak{a}$ 的极小 Gröbner 基 (minimal Gröbner basis).

定义

Gröbner 基 $\mathcal{G} \subseteq \mathcal{K}[\boldsymbol{x}]$ 称为约化 Gröbner 基 (reduced Gröbner basis):

1. $\mathcal{G}$ 中多项式均首一;
2. 对任意 $G \in \mathcal{G}$, G 模 $\mathcal{G} \setminus \{G\}$ 已约化.

定理 (证明 $\Longrightarrow$ 算法 16)

对于给定项序, $\mathcal{K}[\boldsymbol{x}]$ 中非零理想均有唯一的约化 Gröbner 基.

Gröbner 基算法的优化

Buchberger 算法需要计算 S 多项式模多项式集合的范式. 当范式为 0 时, 多项式集合并未改变, 此时的计算实际上是无意义的

$\Longrightarrow$ Buchberger 算法中很多约化均为 0 (Maple 例子)

$\Longrightarrow$ 提前判断该范式是否为 0 的准则将减少 Buchberger 算法的计算量, 从而提高计算效率.

- Buchberger 第一、第二准则: 例如 $\mathrm{lcm}(\mathrm{ht}(F), \mathrm{ht}(G)) = \mathrm{ht}(F)\,\mathrm{ht}(G)$, 第 2.3.5 节
- F_4, F_5 算法: 基于线性代数
- 项序的关键作用: Maple 例子, FGLM 算法
- 程序实现: Buchberger 算法 (绝大多数计算机代数系统); F_4 (FGb 软件包, Maple, Magma)

多项式方程组解的个数

对于多项式组 $\mathcal{F} \subset \mathcal{K}[\boldsymbol{x}]$, 以 $\mathsf{Z}(\mathcal{F})$ 记 $\mathcal{F}$ 在 $\mathcal{K}$ 的代数闭包 $\overline{\mathcal{K}}$ 中的公共零点构成的集合.

多项式方程组到理想

给定 $\mathcal{K}[\boldsymbol{x}] = \mathcal{K}[x_1, \ldots, x_n]$ 中的多项式方程组

$$F_1(\boldsymbol{x}) = 0, \quad \ldots, \quad F_s(\boldsymbol{x}) = 0,$$

称 $\mathcal{F} := \{F_1, \ldots, F_s\}$ 为其定义多项式集合, 并将上述方程组简写为 $\mathcal{F} = 0$.

- 易证 $\mathsf{Z}(\mathcal{F}) = \mathsf{Z}(\langle \mathcal{F} \rangle) \Longrightarrow$ 若 $\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$, 则 $\mathsf{Z}(\mathcal{F}) = \mathsf{Z}(\mathcal{G})$.
- 多项式方程组的解由其定义多项式集合生成的理想 (的根) 唯一确定 $\Longrightarrow$ 转化为对相应理想的研究

多项式方程组解的个数

定理 (Hilbert 弱零点定理) (暂不证明)

设 $\mathcal{K}$ 为代数闭域, $\mathfrak{a}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中理想, 则 $\mathsf{Z}(\mathfrak{a}) = \emptyset$ 当且仅当 $1 \in \mathfrak{a}$.

设方程组 $\mathcal{F} = 0$ 在 $\overline{\mathcal{K}}$ 中有解. 若解的个数有限, 则称该方程组为零维的 (zero-dimensional); 否则称其为正维的 (positive-dimensional).

定理 (不证明)

设 $\mathcal{F} \subseteq \mathcal{K}[\boldsymbol{x}]$, 而 $\mathcal{G}$ 为 $\langle \mathcal{F} \rangle$ 对任给项序的 Gröbner 基, 则下列条件等价:

1. $\mathcal{F} = 0$ 是零维的;
2. 对任意 $1 \leqslant i \leqslant n$, 均存在正整数 m_i 与多项式 $G_i \in \mathcal{G}$ 使得 $\mathrm{ht}(G_i) = x_i^{m_i}$.

- 上述定理与项序的选择无关

多项式方程组解的个数

Example

考虑 $\mathcal{F}=\{x^2+y^2+z^2-4, x^2+2\,y^2-5, xz-1\}$. 首先计算 $\mathcal{F}$ 关于 $x<y<z$ 的字典序 Gröbner 基

$$\mathcal{G}=[x^4-3\,x^2+2, 2\,y^2+x^2-5, 2\,z+x^3-3\,x].$$

显然 $\mathcal{G}$ 满足上述定理的条件, 从而方程组 $\mathcal{F}=0$ 是零维的.

一元方程 $x^4-3\,x^2+2=0$ 有四个解 $x=\pm1, \pm\sqrt{2}$. 将其依次代入 $2\,y^2+x^2-5=0$ 与 $2\,z+x^3-3\,x=0$ 即可求得全部解

$$\left(1, \pm\sqrt{2}, 1\right), \quad \left(-1, \pm\sqrt{2}, -1\right),$$
$$\left(\sqrt{2}, \pm\frac{\sqrt{6}}{2}, \frac{1}{\sqrt{2}}\right), \quad \left(-\sqrt{2}, \pm\frac{\sqrt{6}}{2}, -\frac{1}{\sqrt{2}}\right).$$

利用 Gröbner 基解多项式方程组

现考虑 $\mathfrak{a} = \langle \mathcal{F} \rangle$ 的字典序 Gröbner 基 $\mathcal{G}$. 消元定理说明, $\mathcal{G} \cap \mathcal{K}[\boldsymbol{x}_l]$ 正好是理想 $\mathfrak{a} \cap \mathcal{K}[\boldsymbol{x}_l]$ 的 Gröbner 基, 它反映了 $\mathfrak{a}$ 消去变元 $x_{l+1}, \ldots, x_n$ 后的结果.

给定 l $(1 \leqslant l \leqslant n)$, 并设 $\mathfrak{a}_l$ 为 $\mathfrak{a}$ 的第 l 个消去理想. 若 $\boldsymbol{a} = (a_1, \ldots, a_l) \in \mathsf{Z}(\mathfrak{a}_l)$, 则称 $\boldsymbol{a}$ 为多项式方程组 $\mathcal{F} = 0$ 的一个部分解 (partial solution).

定理 (扩张定理) (不证明)

设 $\mathfrak{a} = \langle F_1, \ldots, F_s \rangle \subseteq \mathbb{C}[\boldsymbol{x}]$, 而 $\mathfrak{a}_{n-1}$ 为理想 $\mathfrak{a}$ 的第 $n-1$ 个消去理想. 对任意 i $(1 \leqslant i \leqslant s)$, 将 F_i 写成如下形式:

$$F_i = G_i\, x_n^{N_i} + H_i,$$

其中 $N_i \geqslant 0$, $G_i \in \mathbb{C}[\boldsymbol{x}_{n-1}]$ 非零, 且 $\deg(H_i, x_n) < N_i$. 又设 $\boldsymbol{c} = (c_1, \ldots, c_{n-1}) \in \mathsf{Z}(\mathfrak{a}_{n-1})$ 为部分解. 若 $\boldsymbol{c} \notin \mathsf{Z}(\{G_1, \ldots, G_s\})$, 则存在 $c_n \in \mathbb{C}$ 使得 $(\boldsymbol{c}, c_n) \in \mathsf{Z}(\mathfrak{a})$.

利用 Gröbner 基解多项式方程组

Example

考虑多项式集合 $\mathcal{F} = \{x^2+y^2+z^2-1, xyz-1\}$, 它在 $x < y < z$ 下的字典序 Gröbner 基为

$$[G_1, G_2] = [x^2y^4 + x^4y^2 - x^2y^2 + 1, z + xy^3 + x^3y - xy].$$

由消元定理知,

$$\mathfrak{a}_1 = \mathfrak{a} \cap \mathbb{C}[x] = \{0\}, \quad \mathfrak{a}_2 = \mathfrak{a} \cap \mathbb{C}[x, y] = \langle G_1 \rangle.$$

1. $\mathfrak{a}_1 = \{0\} \Longrightarrow$ 任意 $a \in \mathbb{C}$ 都是 $\mathcal{F} = 0$ 的部分解.
2. G_1 关于变元 y 的最高项 y^4 的系数为 $x^2 \Longrightarrow$ 当 $a \neq 0$ 时, 存在 $b \in \mathbb{C}$ 使得 (a, b) 也是 $\mathcal{F} = 0$ 的部分解.
3. G_2 关于变元 z 的最高项系数为常数 $\Longrightarrow$ 任意部分解 (a, b) $(a \neq 0)$ 都可以扩张为方程组 $\mathcal{F} = 0$ 的解 (a, b, c).

三角列

吴文俊 (1919–2017)

吴文俊对数学的主要领域——拓扑学做出了重大贡献、开创了崭新的数学机械化领域，获得首届国家最高科技奖、首届国家自然科学一等奖、有东方诺贝尔奖之称的邵逸夫数学奖、国际自动推理最高奖 Herbrand 自动推理杰出成就奖。

- 吴方法, 可用于几何定理机器证明: “This method of Wu completely revolutionized the field, effectively provoking a paradigm shift.” —2006 年邵逸夫奖

三角列：定义

多项式环 $\mathcal{K}[x_1, \ldots, x_n]$: $x_1 < \cdots < x_n$

定义

称有限非空有序集合 $[T_1, \ldots, T_r] \subseteq \mathcal{K}[\boldsymbol{x}]$ 为三角列 (triangular set), 如果 $0 < \mathrm{lv}(T_1) < \cdots < \mathrm{lv}(T_r)$.

$$
\begin{aligned}
&T_1(x_1, \ldots, \boxed{x_{s_1}}) \\
&T_2(x_1, \ldots, x_{s_1}, \ldots, \boxed{x_{s_2}}) \\
&T_3(x_1, \ldots, x_{s_1}, \ldots, x_{s_2}, \ldots, \boxed{x_{s_3}}) \\
&\qquad\qquad \vdots \\
&T_r(x_1, \ldots, x_{s_1}, \ldots, x_{s_2}, \ldots, x_{s_3}, \ldots, \ldots, \boxed{x_{s_r}})
\end{aligned}
$$

$$
\boxed{x_1^2} + x_1 - 2, (x_1 - 2)\boxed{x_2^2} + 3x_1 + 5, (x_1x_2 + x_2 + 2)\boxed{x_4} + x_3^2 + 5x_1 + 2
$$

多元多项式: 从变元的角度/伪除

对 $F \in \mathcal{R}[\boldsymbol{x}] \setminus \mathcal{R}$, 定义 F 的:

- 类 (class): F 所含变元的最大下标 $\mathrm{cls}(F)$
- 导元 (leading variable): $\mathrm{lv}(F) := x_{\mathrm{cls}(F)}$
- 初式 (initial): $\mathrm{ini}(F) := \mathrm{lc}(F, \mathrm{lv}(F))$

伪除公式

设 $F, G \in \mathcal{R}[\boldsymbol{x}]$, $x_k = \mathrm{lv}(G)$, 且 $l = \deg(G, x_k)$, $m = \deg(F, x_k)$.
若 $l > 0$, 则存在 $Q, R \in \mathcal{R}[\boldsymbol{x}]$ 以及整数 $0 \leqslant s \leqslant m - l + 1$ 使得

$$\mathrm{ini}(G)^s F = QG + R, \quad \text{且} \quad \deg(R, x_k) < l.$$

若固定 s, 则 Q, R 唯一确定.

- R: F 对 G 的伪余式 (pseudo-remainder), 记作 $\mathrm{prem}(F, G)$

对三角列的伪除

多项式组的零点

设 $\overline{\mathcal{K}}$ 为 $\mathcal{K}$ 的代数扩域. 对任意集合 $\mathcal{P}, \mathcal{Q} \subseteq \mathcal{K}[\boldsymbol{x}]$, 记:

$$\mathsf{Z}(\mathcal{P}) := \{\bar{\boldsymbol{x}} \in \overline{\mathcal{K}}^n : \ P(\bar{\boldsymbol{x}}) = 0, \forall\, P \in \mathcal{P}\},$$

$$\mathsf{Z}(\mathcal{P}/\mathcal{Q}) := \mathsf{Z}(\mathcal{P}) \setminus \mathsf{Z}(\prod_{Q \in \mathcal{Q}} Q).$$

设 $F \in \mathcal{K}[\boldsymbol{x}]$, $\mathcal{T} = [T_1, \ldots, T_r] \subset \mathcal{K}[\boldsymbol{x}]$ 为三角列，定义 F 关于 $\mathcal{T}$ 的伪余式为

$$\mathrm{prem}(F, \mathcal{T}) := \mathrm{prem}(\cdots \mathrm{prem}(\mathrm{prem}(F, T_r), T_{r-1}), \ldots, T_1).$$

且伪除关系如下 (推导)

$$(\prod_{i=1}^{r} \mathrm{ini}(T_i)^{d_i}) F = \sum_{i=1}^{r} Q_i T_i + \mathrm{prem}(F, \mathcal{T}),$$

- $\mathrm{prem}(F, \mathcal{T})$ 中变元的次数

对三角列的伪除

设 $P, Q \in \mathcal{K}[\boldsymbol{x}]$ 为非零多项式, 且 $Q \notin \mathcal{K}$. 称 P 对 Q 是约化的 (reduced), 如果 $\deg(P, \mathrm{lv}(Q)) < \mathrm{ldeg}(Q)$.

- $\mathrm{prem}(P, Q, \mathrm{lv}(Q))$ 对 Q 是约化的.

设 $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为三角列, 而 P 为任一多项式. 称 P 对 $\mathcal{T}$ 是约化的, 如果 P 对每个 $T \in \mathcal{T}$ 都是约化的.

- $\mathrm{prem}(F, \mathcal{T})$ 对 $\mathcal{T}$ 是约化的.

引理 (证明)

对任意三角列 $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$ 和多项式 $F \in \mathcal{K}[\boldsymbol{x}]$, 若 $\mathrm{prem}(F, \mathcal{T}) = 0$, 则 $\mathsf{Z}(\mathcal{T} / \mathrm{ini}(\mathcal{T})) \subseteq \mathsf{Z}(F)$.

$$(\prod_{i=1}^{r} \mathrm{ini}(T_i)^{d_i}) F = \sum_{i=1}^{r} Q_i T_i + \mathrm{prem}(F, \mathcal{T})$$

特征列

称多项式集合 $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为升列 (ascending set), 如果 $\mathcal{T}$ 是三角列 (不妨设 $\mathcal{T} = [T_1, \ldots, T_r]$) 且 T_i 对所有 T_j 都是约化的, 其中 $1 \leqslant j < i \leqslant r$.

特征列

设 $\mathcal{P} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为非空多项式集合, 称升列 $\mathcal{C} \subseteq \mathcal{K}[\boldsymbol{x}]$ 为 $\mathcal{P}$ 的特征列 (characteristic set), 如果 $\mathcal{C} \subseteq \langle \mathcal{P} \rangle$, 且 $\operatorname{prem}(\mathcal{P}, \mathcal{C}) = \{0\}$.

定理: (证明, 特征列的零点关系)

设 $\mathcal{C} = [C_1, \ldots, C_r]$ 为 $\mathcal{P} \subseteq \mathcal{K}[\boldsymbol{x}]$ 的特征列, 命 $\mathcal{P}_i := \mathcal{P} \cup \{\operatorname{ini}(C_i)\}$ $(i = 1, \ldots, r)$, 而 $\mathcal{I} := \operatorname{ini}(\mathcal{C})$,

$$\mathsf{Z}(\mathcal{C}/\mathcal{I}) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C}), \tag{2}$$

$$\mathsf{Z}(\mathcal{C}/\mathcal{I}) = \mathsf{Z}(\mathcal{P}/\mathcal{I}), \tag{3}$$

$$\mathsf{Z}(\mathcal{P}) = \mathsf{Z}(\mathcal{C}/\mathcal{I}) \cup \bigcup_{i=1}^{r} \mathsf{Z}(\mathcal{P}_i). \tag{4}$$

几何定理机器证明：从一个例子出发

Simson 定理

从任意一点 P 向任意 $\triangle ABC$ 的三边作垂线, 那么垂足 D, E, F 共线当且仅当 P 在 $\triangle ABC$ 的外接圆上.

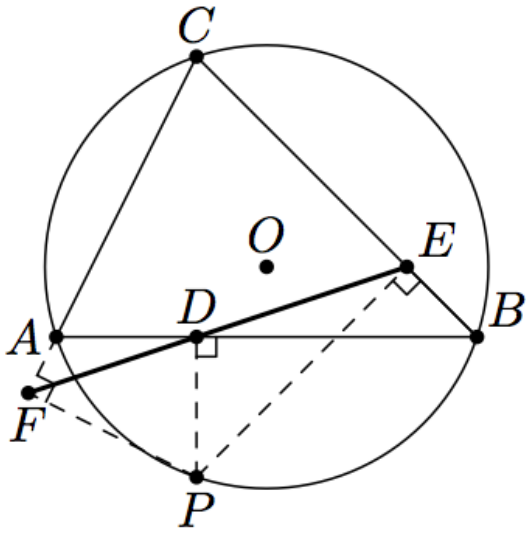


图 6.2　Simson 定理

(只证$\Longleftarrow$)

几何定理机器证明

将几何问题转换为代数问题 $\Longrightarrow$ HOW?

法国哲学家、数学家笛卡尔

把一切问题化为数学问题，把一切数学问题化为代数问题，把一切代数问题化为代数方程求解问题

几何定理机器证明：代数化

坐标化：选取直线 AB 为 x 轴，A, B 的中点为原点，并设各点坐标如下：

$$A(-u_1, 0), \quad B(u_1, 0), \quad C(u_2, u_3), \quad P(y_1, y_2),$$
$$D(y_1, 0), \quad E(y_3, y_4), \quad F(y_5, y_6).$$

假设条件：

$$(\mathcal{H} = 0) \begin{cases} H_1 = u_3 y_2^2 - (u_3^2 + u_2^2 - u_1^2) y_2 + u_3 (y_1^2 - u_1^2) = 0, \\ H_2 = (u_2 + u_1)(y_3 - y_1) + u_3 (y_4 - y_2) = 0, \\ H_3 = (u_2 + u_1) y_4 - u_3 (y_3 + u_1) = 0, \\ H_4 = (u_2 - u_1)(y_5 - y_1) + u_3 (y_6 - y_2) = 0, \\ H_5 = (u_2 - u_1) y_6 - u_3 (y_5 - u_1) = 0. \end{cases}$$

定理结论：$G = (y_3 - y_1) y_6 - y_4 (y_5 - y_1) = 0$

问题化归?

几何定理机器证明：代数化

问题化归

定理成立

$\Downarrow$

满足定理假设条件的任意点，均满足定理结论

$\Downarrow$

假设条件方程组 $\mathcal{H}=0$ 的解均为定理方程 $G=0$ 的解

$\mathrm{Z}(\mathcal{H}) \subset \mathrm{Z}(G)$

已知关于特征列零点的结论

- 设 $\mathcal{C}$ 为 $\mathcal{H}$ 的特征列, 则 $\mathrm{Z}(\mathcal{C}/\mathcal{I}) = \mathrm{Z}(\mathcal{H}/\mathcal{I})$.
- 对于 G, 若 $\mathrm{prem}(G,\mathcal{C}) = 0$, 则 $\mathrm{Z}(\mathcal{C}/\mathcal{I}) \subseteq \mathrm{Z}(G)$.

几何定理机器证明：示例

计算得到特征列如下

$$\mathcal{C} = \left[\begin{array}{l} u_3 y_2^2 + (u_1^2 - u_2^2 - u_3^2) y_2 + u_3 y_1^2 - u_3 u_1^2, \\ I_2 y_3 - I_3^2 y_1 - I_3 u_3 y_2 + u_3^2 u_1, \\ I_3 y_4 - u_3 y_3 - u_3 u_1, \\ I_4 y_5 + I_5^2 y_1 + I_5 u_3 y_2 + u_3^2 u_1, \\ I_5 y_6 - u_3 y_5 + u_3 u_1 \end{array} \right],$$

其中

$$I_2 = u_2^2 + 2\, u_1 u_2 + u_1^2 + u_3^2, \quad I_3 = u_2 + u_1,$$
$$I_4 = u_2^2 - 2\, u_2 u_1 + u_1^2 + u_3^2, \quad I_5 = u_2 - u_1.$$

可以验证, 上述零点关系在 $u_1 u_3 I_2 \cdots I_5 \neq 0$ 的条件下成立: 定理的必要性得证.

几何定理机器证明：示例

退化条件

我们观察下定理成立的条件：$u_1 u_3 I_2 \cdots I_5 \neq 0$

(1) AC 是迷向的 (即 AC 的斜率为 $\pm \mathrm{i}$);

(2) $AB \perp AC$;

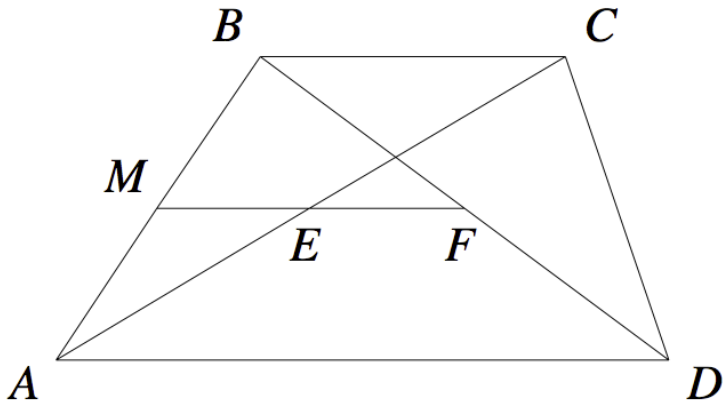
(3) BC 是迷向的;

(4) $AB \perp BC$.

- Maple 程序演示

几何定理机器证明：另一个例子

设梯形 $ABCD$ 的两条对角线之中点的连线 EF 与梯形的一边 AB 相交，那么直线 EF 将线段 AB 平分.



梯形定理

坐标化：

$$A(x_1,0),\quad D(x_2,0),\quad B(x_3,x_4),\quad C(x_5,x_4),$$
$$E(x_6,x_7),\quad F(x_8,x_9),\quad M(x_{10},x_{11}).$$

几何定理机器证明：另一个例子

假设方程组：

$$E \text{ 是 } AC \text{ 的中点} \iff \begin{cases} H_1 = 2\,x_6 - x_5 - x_1 = 0, \\ H_2 = 2\,x_7 - x_4 = 0; \end{cases}$$

$$F \text{ 是 } BD \text{ 的中点} \iff \begin{cases} H_3 = 2\,x_8 - x_3 - x_2 = 0, \\ H_4 = 2\,x_9 - x_4 = 0; \end{cases}$$

$$M \text{ 是 } AB \text{ 和 } EF \text{ 的交点} \iff \begin{cases} H_5 = (x_8 - x_6)\,x_{11} - (x_9 - x_7)\,x_{10} \\ \qquad + x_6 x_9 - x_7 x_8 = 0, \\ H_6 = (x_3 - x_1)\,x_{11} - x_4\,(x_{10} - x_1) = 0. \end{cases}$$

结论方程组：

$$M \text{ 是 } AB \text{ 的中点} \iff \begin{cases} G_1 = 2\,x_{10} - x_3 - x_1 = 0, \\ G_2 = 2\,x_{11} - x_4 = 0. \end{cases}$$

几何定理机器证明：另一个例子

计算特征列:

$$\mathbb{C} = \begin{bmatrix} 2\,x_6 - x_5 - x_1, \\ 2\,x_7 - x_4, \\ 2\,x_8 - x_3 - x_2, \\ 2\,x_9 - x_4, \\ x_4 I\,(2\,x_{10} - x_3 - x_1), \\ (x_3 - x_1)\,I\,(2\,x_{11} - x_4) \end{bmatrix},$$

其中,

$$I = x_5 - x_3 - x_2 + x_1.$$

验证: $\mathrm{prem}(G_1, \mathbb{C}) = \mathrm{prem}(G_2, \mathbb{C}) = 0.$

退化条件: $x_4(x_3 - x_1)I \neq 0$

几何定理机器证明

问题可以归结为判定包含关系 $\mathsf{Z}(\mathcal{H}) \subseteq \mathsf{Z}(G)$ 是否成立. 这一关系一般来说并不成立, 于是我们需要确定一组条件, 使得 $\mathsf{Z}(\mathcal{H}) \subseteq \mathsf{Z}(G)$ 在该条件之下成立. 所确定的条件通常正好排除了定理的退化情形.

几何定理机器证明的原理

设等式型定理的假设和结论分别为 $\mathcal{H} = 0$ 和 $G = 0$, $\mathcal{C}$ 为 $\mathcal{H}$ 关于变元序 $x_1 < \cdots < x_n$ 的特征列, 而 $I = \prod_{C \in \mathcal{C}} \mathrm{ini}(C)$. 若 $\mathrm{prem}(G, \mathcal{C}) \equiv 0$, 则 $\mathsf{Z}(\mathcal{H}/I) \subseteq \mathsf{Z}(G)$, 因此定理在条件 $I \neq 0$ 之下成立.

问题

利用吴方法进行几何定理机器证明中 $\mathrm{prem}(F, \mathcal{C}) \neq 0$ 怎么办?

- 需要对 $\mathcal{H}$ 的零点进行更加精细的描述 $\Longrightarrow$ 三角分解

吴特征列算法：秩

将 $F \in \mathcal{K}[\boldsymbol{x}]$ 中出现的最大变元的下标称作 F 的类, 记作 $\mathrm{cls}(F)$.

多项式的秩

设 $P, Q \in \mathcal{K}[\boldsymbol{x}]$ 为非零多项式, 称 P 的秩低于 Q 的秩, 记为 $P \prec Q$, 如果下列条件之一成立:

1. $P \in \mathcal{K}$, 而 $Q \notin \mathcal{K}$; (多项式大于常数)
2. $P, Q \notin \mathcal{K}$, 且 $\mathrm{cls}(P) < \mathrm{cls}(Q)$; (类大的大于类小的)
3. $P, Q \notin \mathcal{K}$, $\mathrm{cls}(P) = \mathrm{cls}(Q)$, 且 $\mathrm{ldeg}(P) < \mathrm{ldeg}(Q)$. (看次数)

- $P \sim Q$: 如果 $P \prec Q$ 和 $Q \prec P$ 都不成立
- $P \precsim Q$: $P \prec Q$ 或 $P \sim Q$

- 上述定义的 $\precsim$ 是一个偏序关系: 自反性、传递性、反对称性

吴特征列算法：三角列的秩

三角列的秩

设 $\mathcal{T} = [T_1, \ldots, T_r]$ 和 $\mathcal{S} = [S_1, \ldots, S_t]$ 为三角列, 称 $\mathcal{T}$ 的秩低于 $\mathcal{S}$ 的秩, 记为 $\mathcal{T} \prec \mathcal{S}$, 如果下列条件之一成立:

1. 存在 $i \leqslant \min(r, t)$, 对每个 $j < i$ 有 $T_j \sim S_j$, 而 $T_i \prec S_i$ 成立;
2. $r > t$, 且对每个 $j \leqslant t$ 都有 $T_j \sim S_j$ 成立.

引理 (证明)

设 $\mathcal{T} = [T_1, \ldots, T_r]$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的升列, $P \in \mathcal{K}[\boldsymbol{x}] \setminus \mathcal{K}$. 若 $\mathcal{T}$ 是非平凡的, 且 P 对 $\mathcal{T}$ 是约化的, 则 $[\mathcal{T}_{<\mathrm{lv}(P)}, P] \prec \mathcal{T}$.

- 其中 $\mathcal{T}_{<x_k}$ 为 $\mathcal{T}$ 中导元 $< x_k$ 的多项式所构成的截断三角列.

吴特征列算法：基列

定义：基列

对任意非空有限多项式集合 $\mathcal{P} \subseteq \mathcal{K}[\boldsymbol{x}]$, 设 Φ 为所有包含于 $\mathcal{P}$ 的升列组成的集合 (显然非空). 称 Φ 的任意极小升列 (即关于 $\prec$ 秩最低的升列) 为 $\mathcal{P}$ 的基列 (basic set).

- 基列不唯一, 易证若 $\mathcal{B}_1$ 和 $\mathcal{B}_2$ 都是 $\mathcal{P}$ 的基列, 则 $\mathcal{B}_1 \sim \mathcal{B}_2$

构造基列

命 $\mathcal{F}_1 := \mathcal{P}$, 并设 B_1 为 $\mathcal{F}_1$ 中秩最低的多项式. 若 B_1 为非零常数, 则 $[B_1]$ 是 $\mathcal{P}$ 的一个基列. 否则, 命

$$\mathcal{F}_2 := \{F \in \mathcal{F}_1 \setminus \{B_1\} : F \text{ 对 } B_1 \text{ 是约化的}\}.$$

若 $\mathcal{F}_2 = \emptyset$, 则 $[B_1]$ 是 $\mathcal{P}$ 的一个基列. 否则, 设 B_2 为 $\mathcal{F}_2$ 中秩最低的多项式. 易知 $B_1 \prec B_2$ ($\mathrm{lv}(B_2) = ?$)

- $[B_1] \succ [B_1, B_2]$.

吴特征列算法：基列的计算

算法 11 基列算法 $\mathcal{B}$:=BasSet($\mathcal{P}$, ord)

输入: 有限非空多项式集合 $\mathcal{P} \subseteq \mathcal{K}[\boldsymbol{x}]$, 变元序 ord $= x_1 < \cdots < x_n$.

输出: $\mathcal{P}$ 的基列 $\mathcal{B}$.

$\mathcal{B} := \emptyset; \mathcal{F} := \mathcal{P};$

while $\mathcal{F} \neq \emptyset$ **do**

  $F :=$ $\mathcal{F}$ 中秩最低的多项式;

  $\mathcal{B} := [\mathcal{B}, F]$; /* 若 $\mathcal{B} = [B_1, \ldots, B_r]$, 则 $[\mathcal{B}, F] = [B_1, \ldots, B_r, F]$. */

  if $\mathrm{cls}(F) = 0$ **then** $\mathcal{F} := \emptyset$;

  else $\mathcal{F} := \{G \in \mathcal{F} \backslash \{F\} : G$ 对 F 是约化的$\}$;

end

return $\mathcal{B}$;

- 终止性: 因为 $\mathcal{P}$ 是有限的而基列或者只含一个非零常数, 或者作为三角列至多含有 n 个多项式.

吴特征列算法：特征列的计算

算法 12 吴特征列算法 $\mathcal{C} := \mathsf{CharSet}(\mathcal{P}, \mathrm{ord})$

输入: 非空有限多项式集合 $\mathcal{P} \subseteq \mathcal{K}[\boldsymbol{x}]$, 变元序 $\mathrm{ord} = x_1 < \cdots < x_n$.

输出: $\mathcal{P}$ 的特征列 $\mathcal{C}$.

$\mathcal{F} := \mathcal{P}; \mathcal{R} := \mathcal{P};$

while $\mathcal{R} \neq \emptyset$ **do**

  $\mathcal{C} := \mathsf{BasSet}(\mathcal{F}, \mathrm{ord});$

  if $\mathcal{C} \cap \mathcal{K} \neq \emptyset$ **then** $\mathcal{R} := \emptyset;$

  else $\mathcal{R} := \{\mathrm{prem}(F, \mathcal{C}) : F \in \mathcal{F} \setminus \mathcal{C}\} \setminus \{0\};$

  $\mathcal{F} := \mathcal{P} \cup \mathcal{C} \cup \mathcal{R};$

end

return $\mathcal{C}$;

- 证明: 正确性和终止性 (引理)
- VS Buchberger 算法?

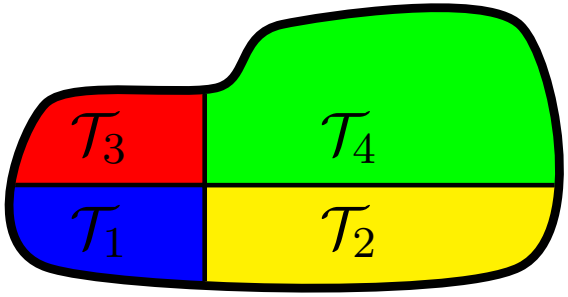
三角分解

多项式组 $\mathcal{P} \subset \mathcal{K}[x_1, \ldots, x_n]$

$\Downarrow$

三角列 $\mathcal{T}_1, \ldots, \mathcal{T}_r$

使得 $\mathsf{Z}(\mathcal{P}) = \bigcup_{i=1}^{r} \mathsf{Z}(\mathcal{T}_i / \operatorname{ini}(\mathcal{T}_i))$



三角分解

- 吴文俊: 特征列 $\hookrightarrow$ 伪除
- 王东明: 不可约三角列、简单列 $\hookrightarrow$ 因式分解, 无平方分解
- 杨路-张景中: 真升列 $\hookrightarrow$ 结式
- M. Kalkbrener: 正则链 $\hookrightarrow$ 零因子

特征分解

定理 (特征列的零点关系)

设 $\mathcal{C} = [C_1, \ldots, C_r]$ 为 $\mathcal{P} \subseteq K[\boldsymbol{x}]$ 的特征列, 命 $\mathcal{P}_i := \mathcal{P} \cup \{\mathrm{ini}(C_i)\}$ $(i = 1, \ldots, r)$, 而 $\mathcal{I} := \mathrm{ini}(\mathcal{C})$,

$$\mathsf{Z}(\mathcal{C}/\mathcal{I}) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C}),$$
$$\mathsf{Z}(\mathcal{C}/\mathcal{I}) = \mathsf{Z}(\mathcal{P}/\mathcal{I}),$$
$$\mathsf{Z}(\mathcal{P}) = \mathsf{Z}(\mathcal{C}/\mathcal{I}) \cup \bigcup_{i=1}^{r} \mathsf{Z}(\mathcal{P}_i).$$

- $\mathcal{C} \subseteq \langle \mathcal{P} \rangle \subseteq \langle \mathcal{P}_i \rangle \Longrightarrow \mathsf{Z}(\mathcal{P}_i) \subseteq \mathsf{Z}(\mathcal{C}) \Longrightarrow \mathsf{Z}(\mathcal{P}_i \cup \mathcal{C}) = \mathsf{Z}(\mathcal{P}_i)$
- 应用吴特征列算法计算每个 $\mathcal{P}_i \cup \mathcal{C}$ 的特征列, 重复可得:

$$\mathsf{Z}(\mathcal{P}) = \bigcup_{i=1}^{s} \mathsf{Z}(\mathcal{C}_i/\mathcal{I}_i)$$

不可约分解：示例

$$\mathcal{P} = [(x_1+1)(x_1-2), (x_1-2){x_2}^2 + x_2 + 2x_1^2,$$
$$(x_1+x_2){x_3}^3 + x_2x_3^2 + x_1x_2 + 3]$$

$$\Downarrow$$

$$\mathcal{T}_1 = [x_1+1, 3x_2+2, 5x_3^3 + 2x_3^2 - 11]$$
$$\mathcal{T}_2 = [x_1-2, x_2+8, 6x_3^3 + 8x_3^2 + 13]$$
$$\mathcal{T}_3 = [x_1+1, x_2-1, x_3^2+2]$$

- $\mathcal{T}_i$ 中的多项式: 不可约
- 方法: 多项式在代数扩域上的因式分解

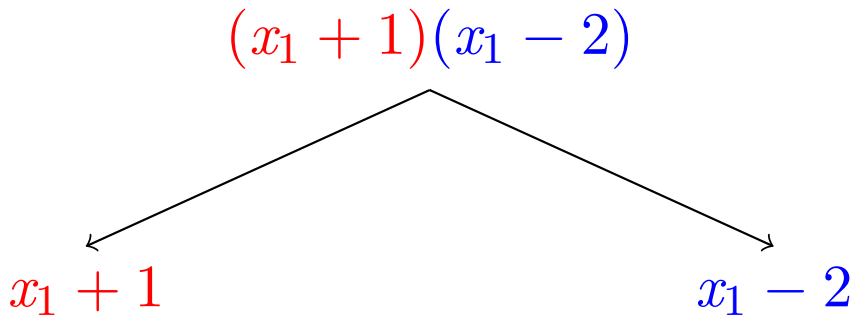
不可约分解：示例

$$(x_1+1)(x_1-2), (x_1-2)x_2^2+x_2+2x_1^2, (x_1+x_2)x_3^3+x_2x_3^2+x_1x_2+3$$

$$(x_1+1)(x_1-2)$$

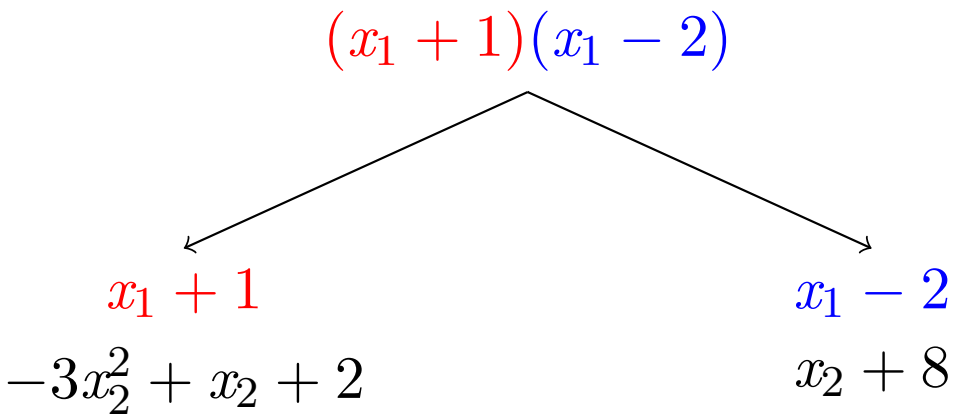
不可约分解：示例

$$(x_1+1)(x_1-2), (x_1-2)x_2^2+x_2+2x_1^2, (x_1+x_2)x_3^3+x_2x_3^2+x_1x_2+3$$



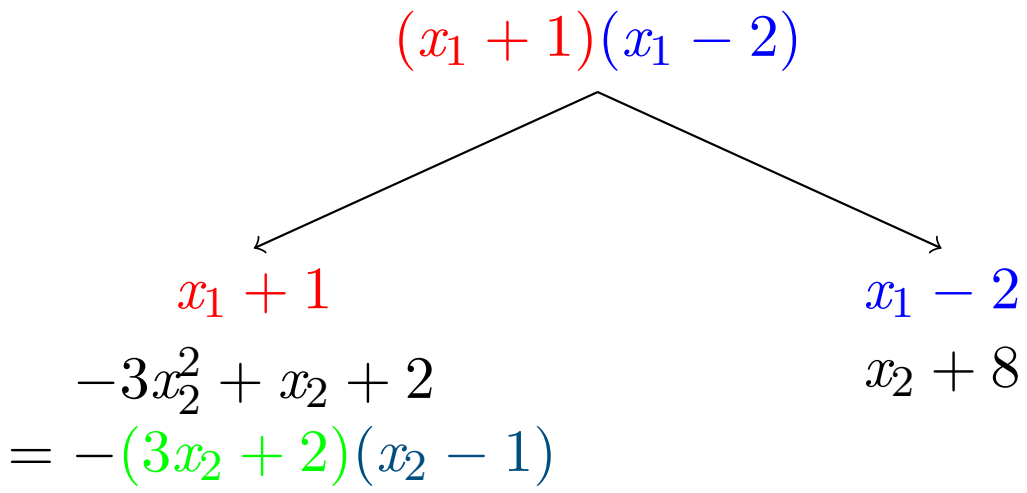
不可约分解：示例

$$(x_1+1)(x_1-2), (x_1-2)x_2^2+x_2+2x_1^2, (x_1+x_2)x_3^3+x_2x_3^2+x_1x_2+3$$



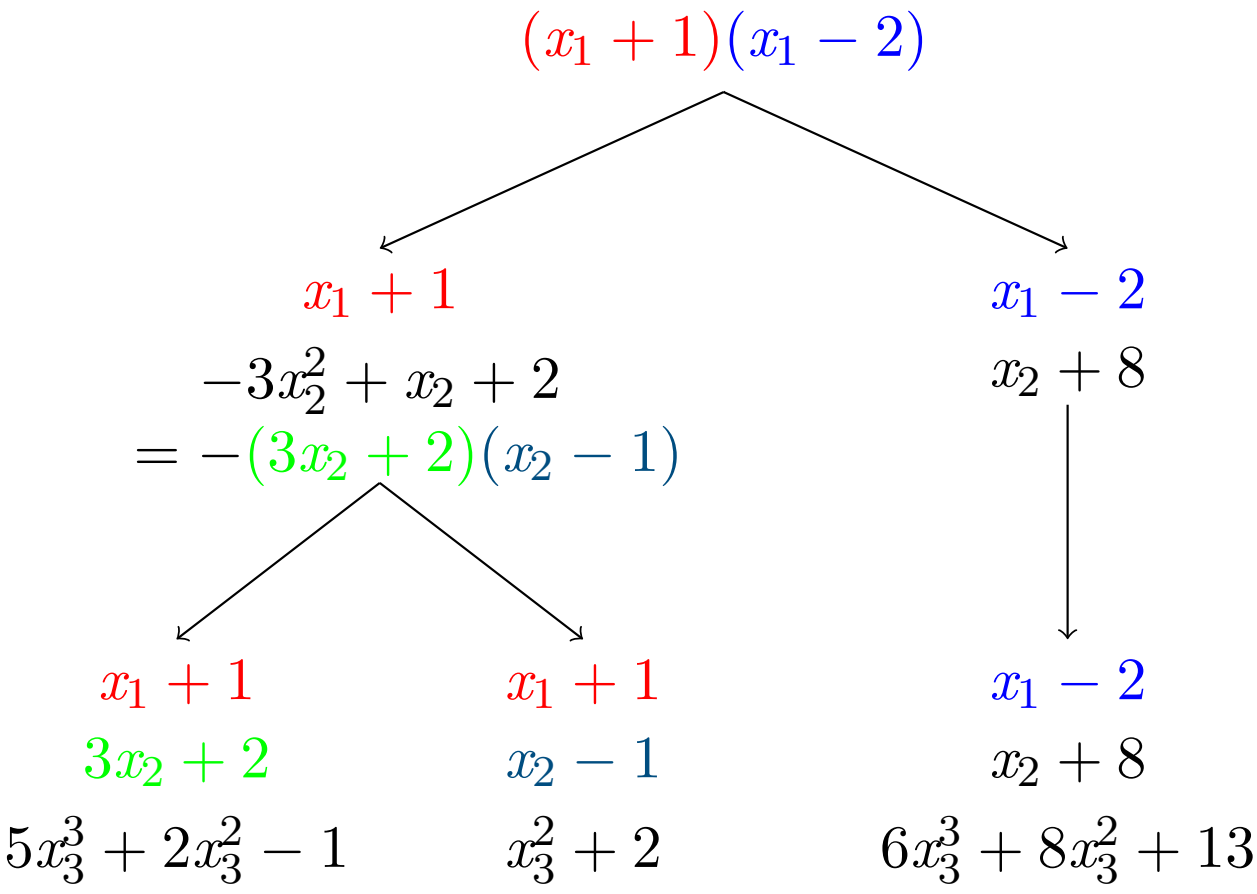
不可约分解：示例

$$(x_1+1)(x_1-2), (x_1-2)x_2^2+x_2+2x_1^2, (x_1+x_2)x_3^3+x_2x_3^2+x_1x_2+3$$



不可约分解：示例

$$(x_1+1)(x_1-2),\ (x_1-2)x_2^2+x_2+2x_1^2,\ (x_1+x_2)x_3^3+x_2x_3^2+x_1x_2+3$$



各种三角列

三角列本身的定义要求很低，但通常我们会对三角列中的多项式添加更多的限制以使得三角列具备更好的性质，如不可约三角列、$\mathsf{Z}(\mathcal{T}/\operatorname{ini}(\mathcal{T})) \neq \emptyset$.

设 $\mathcal{T} = [T_1, \ldots, T_r] \subset \mathcal{K}[\boldsymbol{x}]$ 为三角列

- 正则列：每个 $\operatorname{ini}(T_i)$ 在代入 $T_1, \ldots, T_{i-1}$ 的解后$\neq 0$
- 简单列：每个 T_i 在代入 $T_1, \ldots, T_{i-1}$ 的解后无平方
- 不可约三角列: 每个 T_i 在代入 $T_1, \ldots, T_{i-1}$ 的解后不可约
- 正规列: 每个 $\operatorname{ini}(T_i)$ 仅含参量