

符号计算及应用

牟晨琪

北京航空航天大学
数学科学学院

chenqi.mou@buaa.edu.cn

2023 年 4–5 月
北京师范大学短课程

符号计算：从一个例子开始

JOHN D. COOK
CONSULTING

ABOUT SERVICES WRITING CLIENTS

(832) 422-8646

CONTACT

Solving systems of polynomial equations

Posted on 13 May 2017 by John

In a high school algebra class, you learn how to solve polynomial equations in one variable, and systems of linear equations. You might reasonably ask "So when do we combine these and learn to solve systems of polynomial equations?" The answer would be "Maybe years from now, but most likely never." There are systematic ways to solve systems of polynomial equations, but you're unlikely to ever see them unless you study algebraic geometry.

Here's an example from [1]. Suppose you want to find the extreme values of $x^3 + 2xyz - x^2$ on the unit sphere using Lagrange multipliers. This leads to the following system of polynomial equations where λ is the Lagrange multiplier.

$$\begin{aligned} 3x^2 + 2yz - 2x\lambda &= 0 \\ 2xz - 2y\lambda &= 0 \\ 2xy - 2z - 2z\lambda &= 0 \\ x^2 + y^2 + z^2 - 1 &= 0 \end{aligned}$$

🔍



[LET'S TALK](#)

Latest Posts

[Discrete example of concentration of measure](#)

[Nearly all the area in a high-dimensional sphere is near the equator](#)

- **Maple 例子：**上面截图中曲面方程应为 $x^3 + 2xyz - z^2$

解多项式方程组

Example

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

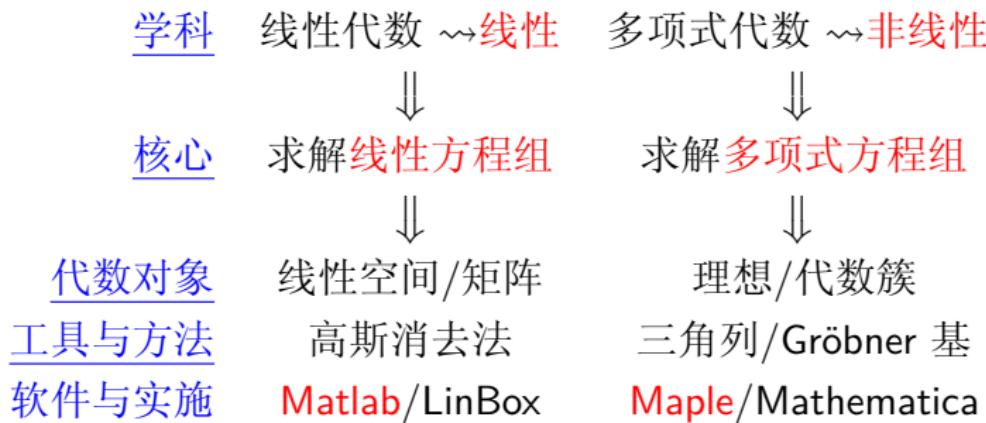
$$\begin{cases} x_1 + x_2 + \cdots + x_n = 0, \\ x_1 x_2 + x_2 x_3 + \cdots + x_n x_1 = 0, \\ \cdots \\ x_1 x_2 \cdots x_n - 1 = 0. \end{cases}$$

- $n = 8$: >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 $\mathcal{F} \subseteq \mathcal{K}[\mathbf{x}]$ 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?

符号计算 = 计算机代数

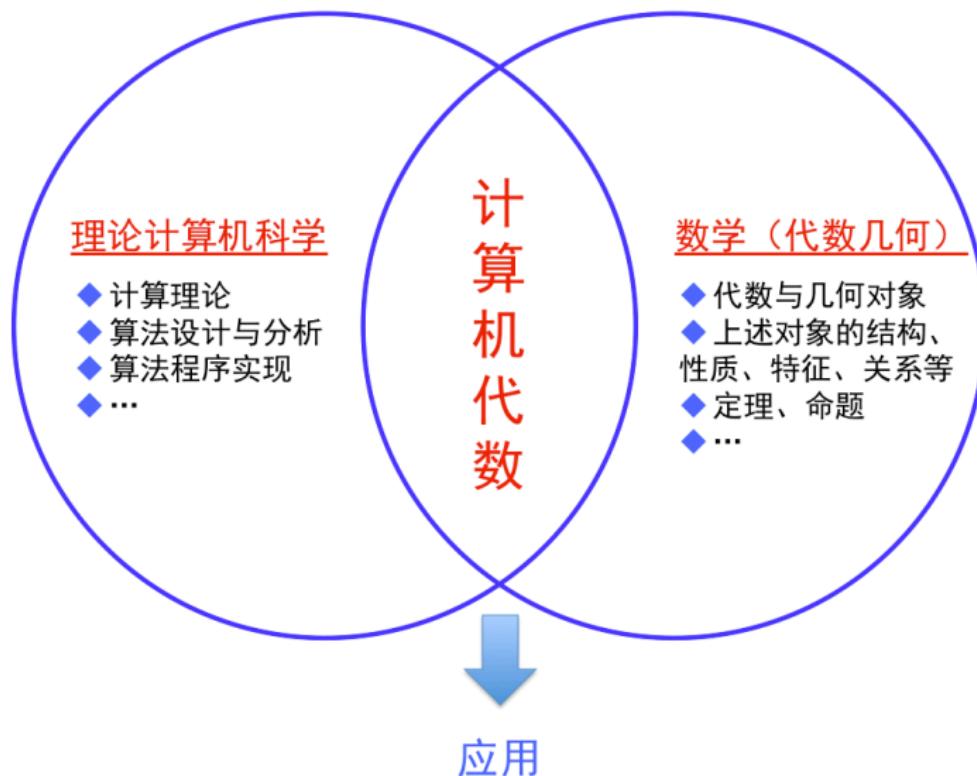


符号计算 (VS 数值计算)

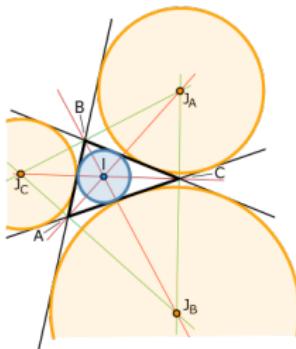
符号计算又称计算机代数，主要处理具有含义的抽象符号，主要研究如何进行这些符号之间的精确运算，因而**没有误差**。

- **数值计算**: 有误差、数值稳定性、收敛速度、计算效率
- (理论) 数学中的运算都是符号运算: 如**高斯消去法**

符号计算：交叉学科



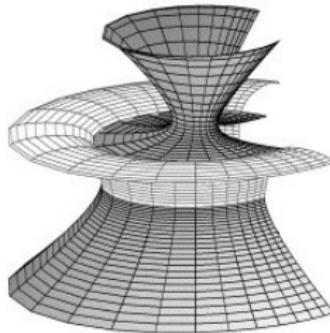
符号计算：应用



几何定理的机器证明



机器人运动学



曲线与曲面的计算



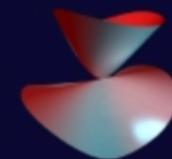
密码学

代数曲面

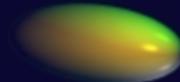
Calyx
 $x^2+y^2z^3 = z^4$



Calypso
 $x^2+y^2z = z^2$



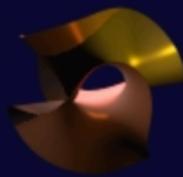
Dattel
 $3x^2+3y^2+z^2=1$



Daisy
 $(x^2 - y^3)^2 = (z^2 - y^2)^3$



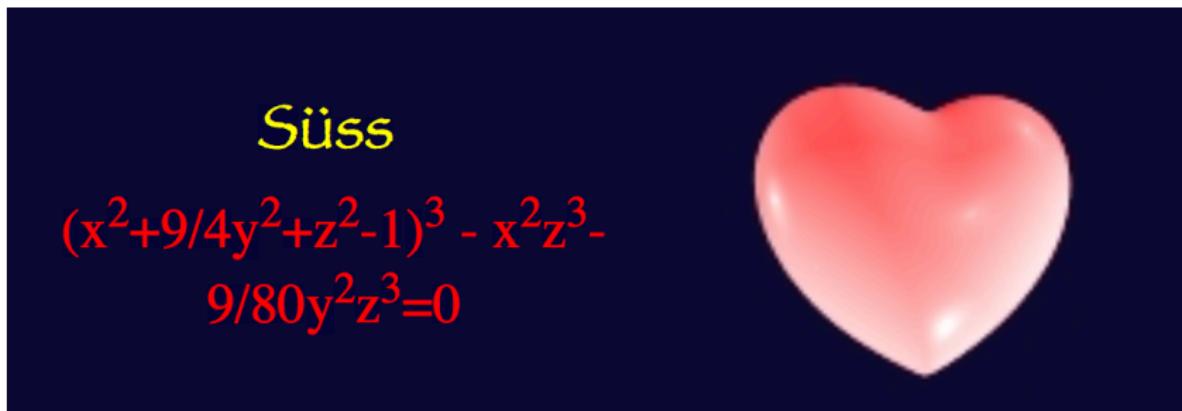
Durchblick
 $x^3y+xz^3+y^3z+z^3+5z = 0$



Eistüte
 $(x^2+y^2)^3 = 4x^2y^2(z^2+1)$



代数曲面



- 做图
- 多项式 VS 曲面 \implies 代数表达式 VS 几何表示
- 隐式表示 VS 显示表示

更多代数曲面: <http://homepage.univie.ac.at/herwig.hauser/bildergalerie/gallery.html>

课程基本内容

① 引言

- 多项式基础

② 结式

- 基于线性代数的消元方法

③ Gröbner 基

- 符号计算最核心的方法，应用广泛

④ 三角列

- 几何定理机器证明

⑤ 柱形代数分解

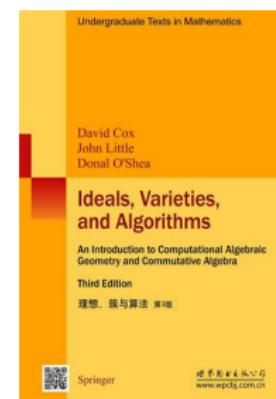
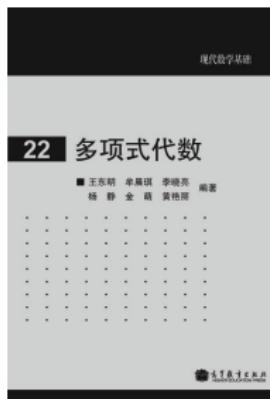
- 实系数 + 不等式、一元多项式的实根隔离

⑥ 其他应用（时间允许的话）

- 微分系统的定性分析

课程参考书目

- 《多项式代数》：王东明，牟晨琪等，高等教育出版社
- 《计算机代数》：王东明，夏壁灿，李子明，清华大学出版社
- 《Ideals, Varieties, and Algorithms》：D. Cox, J. Little, D. O’Shea, Springer (已引进，《理想、簇与算法》)



课程资源

课件：个人主页 (cmou.net) → 左上角点击“中文”→ 课程

计算机代数课程视频

3323播放 · 49弹幕 2020-02-22 21:07:01



北航牟老师
发消息

健康快乐地学习

+ 关注 104
收起

弹幕列表 :

时间	弹幕内容 (23)	发送时间
00:16	老师好，老师辛苦啦，老师...	02-23 21:09
00:46	6666	02-23 21:09
00:24	好好学习天天向上	02-24 10:05
04:23	北邮学子慕名而来	02-24 15:23
00:45	李宗琳说他裂开了	02-25 11:14
00:00	萌	02-25 20:17
03:05	666	02-26 08:04
33:46	喜欢的女同学的心事话筒hhh	02-23 23:30
12:00	那么问题来了，什么样的多...	02-23 23:18
36:26	画一半把笔一掉：分手吧	02-27 12:32
38:49	在代数与几何之间反复横跳	02-23 23:35
41:23	maple 不好使	08-08 17:18
41:29	用Python的sympy吧！	09-19 10:58
08:05	肖克裂开了	02-25 11:20
08:22	裂了	02-26 16:28
09:20	高斯消元	02-23 23:16
09:36	弹幕这么少	02-25 18:31
10:59	高潮 已经很简单了	07-27 12:41
80:21	没有看到这的人吧	02-28 18:31
81:43	I	02-26 19:10
81:50	应该是 $\alpha_i < \beta_j$ 吧？	09-09 09:46
92:37	好抽象啊	09-09 10:00
92:34	我李宗琳竟然看完了	02-25 12:58

- Bilibili 网站: 搜索“计算机代数”
- 牟晨琪: chenqi.mou@buaa.edu.cn

多项式基础

多项式

设 \mathcal{R} 为带单位元的交换环, x_1, \dots, x_n 为 \mathcal{R} 上的未定元.

称形式幂积 $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ ($\alpha_i \geq 0$) 为关于 x_1, \dots, x_n 的项 (term), 简记为 \mathbf{x}^α , 其中 \mathbf{x} 和 α 分别表示向量 (x_1, \dots, x_n) 和 $(\alpha_1, \dots, \alpha_n)$.

- α_i 为 \mathbf{x}^α 关于变元 x_i 的次数 (degree), 记为 $\deg(\mathbf{x}^\alpha, x_i)$
- $\alpha_1 + \cdots + \alpha_n$ 为 \mathbf{x}^α 的全次数 (total degree), 记为 $\operatorname{tdeg}(\mathbf{x}^\alpha)$.

称有限和 $F = \sum_{\alpha} c_{\alpha} x^{\alpha}$ ($c_{\alpha} \in \mathcal{R}$) 为 \mathcal{R} 上关于 x_1, \dots, x_n 的多项式 (polynomial)

- c_{α} 为 F 关于项 \mathbf{x}^α 的系数 (coefficient), 记为 $\operatorname{coef}(F, \mathbf{x}^\alpha)$
- 若 $c_{\alpha} \neq 0$, 则称 $c_{\alpha} x^{\alpha}$ 为 F 的单项式 (monomial).
- F 关于变元 x_i 的次数 (degree)

$$\deg(F, x_i) := \max\{\deg(\mathbf{x}^\alpha, x_i) : \operatorname{coef}(F, \mathbf{x}^\alpha) \neq 0\}$$

- F 的全次数 (total degree)

$$\operatorname{tdeg}(F) := \max\{\operatorname{tdeg}(\mathbf{x}^\alpha) : \operatorname{coef}(F, \mathbf{x}^\alpha) \neq 0\}$$

多项式环

对于 \mathcal{R} 上关于 x_1, \dots, x_n 的任意多项式 $F = \sum_{\alpha} a_{\alpha} x^{\alpha}$, $G = \sum_{\alpha} b_{\alpha} x^{\alpha}$, 定义加法和乘法如下:

$$F + G := \sum_{\alpha} (a_{\alpha} + b_{\alpha}) x^{\alpha}, \quad F \cdot G := \sum_{\gamma} c_{\gamma} x^{\gamma},$$

其中 $c_{\gamma} = \sum_{\alpha+\beta=\gamma} a_{\alpha} b_{\beta}$.

按上述定义的加法和乘法, \mathcal{R} 上关于 x_1, \dots, x_n 的所有多项式组成的集合构成带单位元的交换环, 称为 \mathcal{R} 上关于 x_1, \dots, x_n 的多项式环 (polynomial ring), 记为 $\mathcal{R}[x_1, \dots, x_n]$ 或 $\mathcal{R}[x]$.

- 当 $n = 1$ 时, 称为一元多项式环 (univariate polynomial ring);
- 当 $n > 1$ 时, $\mathcal{R}[x]$ 称为多元多项式环 (multivariate polynomial ring).

域上的一元多项式

设 \mathcal{K} 为域, $F \in \mathcal{K}[x]$, 将 $\deg(F, x)$ 和 $\text{lc}(F, x)$ 简记为 $\deg(F)$ 和 $\text{lc}(F)$.

定理

设 \mathcal{K} 为域, G 为 $\mathcal{K}[x]$ 中的非常数多项式, 则对任意 $F \in \mathcal{K}[x]$, 存在唯一的 $Q, R \in \mathcal{K}[x]$ 使得

$$F = QG + R,$$

其中 $\deg(R) < \deg(G)$.

若上述定理中的条件满足, 则称上式为 F 关于 G 的带余除法公式 (division formula), 而 Q 和 R 分别为 F 关于 G 的商 (quotient) 和余式 (remainder).

带余除法算法

例: $x^3 + 2x + 1$ 除以 $2x + 3 \in \mathbb{Q}[x]$

算法 2 带余除法 $(Q, R) := \text{Rem}(F, G)$

输入: 多项式 $F, G \in \mathcal{K}[x]$.

输出: F 关于 G 的商 Q 和余式 R .

$Q := 0; R := F; l := \deg(G);$

while $\deg(R) \geq l$ **do**

$r := \deg(R);$

$R := R - (\text{lc}(R)/\text{lc}(G))x^{r-l}G;$

$Q := Q + (\text{lc}(R)/\text{lc}(G))x^{r-l};$

end

return $(Q, R);$

Euclid 算法：域上的一元多项式

算法 3 Euclid 算法 $(H, A, B) := \text{Euclid}(F, G)$

输入: 多项式 $F, G \in \mathcal{K}[x]$.

输出: F 和 G 的最大公因子 H , 以及 A 和 B , 使得 $H = AF + BG$.

```

1  $H := F; L := G; U := 0; V := 1; A := 1; B := 0;$ 
2 while  $L \neq 0$  do
3    $(Q, R) := \text{Rem}(H, L);$ 
4    $H := L; L := R;$ 
5    $C := A; D := B;$ 
6    $A := U; B := V;$ 
7    $U := C - QU; V := D - QV;$ 
8 end
9 return  $(H, A, B);$ 
```

- **扩展的 Euclid 算法:** 同时输出 $A, B \in \mathcal{K}[x]$ 使得 $H = AF + BG$
- **证明:** 终止性 / 输出 H 是最大公因子

结式

结式：用根定义

考虑两个多项式

$$F = \sum_{i=0}^m a_i x^i, \quad G = \sum_{j=0}^l b_j x^j \in \mathcal{R}[x]$$

其中 $a_m, b_l \neq 0$, 且 $m, l > 0$.

一元结式

$F, G \in \mathcal{R}[x]$ 关于 x 的结式 (resultant) 定义为

$$\text{Res}(F, G, x) := a_m^l b_l^m \prod_{i=1}^m \prod_{j=1}^l (\alpha_i - \beta_j),$$

其中 α_i ($1 \leq i \leq m$) 和 β_j ($1 \leq j \leq l$) 分别为 F 和 G 的根.

- $\text{Res}(F, G, x) = 0$ 当且仅当 F 和 G 有公共根

Sylvester 结式

Sylvester 矩阵

称 $m + l$ 阶方阵

$$\left(\begin{array}{cccccc} a_m & a_{m-1} & \cdots & a_0 & & \\ \ddots & \ddots & \ddots & \ddots & & \\ & a_m & a_{m-1} & \cdots & a_0 & \\ b_l & b_{l-1} & \cdots & b_0 & & \\ \ddots & \ddots & \ddots & \ddots & & \\ & b_l & b_{l-1} & \cdots & b_0 & \end{array} \right) \left. \begin{array}{c} l \\ m \end{array} \right\}$$

为 F 和 G 关于 x 的 **Sylvester** (西尔维斯特) 矩阵, 记作 $\text{Syl}(F, G, x)$.

- $\text{Syl}(F, G, x)$ 的前 l 行: $x^{l-1}F, \dots, xF, F$ 的系数 (后面行)

Sylvester 结式

称矩阵 $\text{Syl}(F, G, x)$ 的行列式为 F 和 G 关于 x 的 **Sylvester 结式**,
记作 $\text{res}(F, G, x) \implies \in$ 哪里?

Sylvester 结式

$$\text{res}(\mathbf{G}, \mathbf{F}, x) = (-1)^{ml} \det(\text{Syl}(F, G, x)) = (-1)^{ml} \text{res}(\mathbf{F}, \mathbf{G}, x)$$

Example

$F = x^3 + 3x - 1, \quad G = F' = 3x^2 + 3,$ 则

$$\text{res}(F, G, x) = \det \begin{pmatrix} 1 & 0 & 3 & -1 & 0 \\ 0 & 1 & 0 & 3 & -1 \\ 3 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 3 \end{pmatrix} = 135,$$

且 $\text{res}(G, F, x) = (-1)^6 \text{res}(F, G, x) = 135.$

- $\text{res}(F, G, x)$ VS $\text{Res}(F, G, x)?$

结式的性质 I

命题 (证明)

设 $F, G \in \mathcal{R}[x]$ 如前所示, 则存在 $A, B \in \mathcal{R}[x]$, 使得 $AF + BG = \text{res}(F, G, x)$, 且 $\deg(A) < l, \deg(B) < m$.

将 Sylvester 矩阵的第 i 列乘以 x^{m+l-i} 然后加到最后一列, 变为

$$\left(\begin{array}{cccccc|c} a_m & a_{m-1} & \cdots & a_0 & & & x^{l-1} F \\ \ddots & \ddots & \ddots & \ddots & & & \\ & a_m & a_{m-1} & \cdots & & & F \\ b_l & b_{l-1} & \cdots & b_0 & & & x^{m-1} G \\ \ddots & \ddots & \ddots & \ddots & & & \\ & b_l & b_{l-1} & \cdots & & & G \end{array} \right) \left. \begin{array}{l} \\ \\ \\ \\ \\ \end{array} \right\} l \left. \begin{array}{l} \\ \\ \\ \\ \\ \end{array} \right\} m$$

将上述矩阵的行列式按最后一列展开即证.

- 矩阵的第 3 类初等变换, 不改变行列式

结式的性质 II

命题 (证明)

设 $F, G \in \mathcal{R}[x]$ 如前文所示, 则下列条件等价:

- ① $\text{res}(F, G, x) = 0$;
- ② 存在非零多项式 $A, B \in \mathcal{R}[x]$, 使得 $AF + BG = 0$,
且 $\deg(A) < l, \deg(B) < m$.
- 线性方程组是否有非零解

推论 (证明、结式的重要性质)

设 $F, G \in \mathcal{R}[x]$ 如前文所示, 则 $\text{res}(F, G, x) = 0$ 当且仅当 F 和 G 有非常数公因子.

- VS $\text{Res}(F, G, x) (= 0$ 当且仅当有公共根)?

结式的应用: 解多项式方程组

圆与椭圆的交点问题

$$\begin{cases} P_1 = x_1^2 + x_2^2 - 2 = 0 \\ P_2 = x_1^2 + 6x_2^2 - 3 = 0 \end{cases}$$

- ① 计算 P_1 与 P_2 关于 x_1 的结式

$$R = \text{res}(P_1, P_2, x_1) = (5x_2^2 - 1)^2. \quad \text{有公共根等价于?}$$

- ② 计算 R 关于 x_2 的解得 $x_2 = \pm \frac{1}{\sqrt{5}}$.

- ③ 分别代入 $P_1 = 0$ 与 $P_2 = 0$, 则两式均变为 $x_1^2 - \frac{9}{5} = 0$, 解得 $x_1 = \pm \frac{3}{\sqrt{5}}$.

所有解

$$\left(\frac{3}{\sqrt{5}}, \frac{1}{\sqrt{5}} \right), \left(\frac{3}{\sqrt{5}}, -\frac{1}{\sqrt{5}} \right), \left(-\frac{3}{\sqrt{5}}, \frac{1}{\sqrt{5}} \right), \left(-\frac{3}{\sqrt{5}}, -\frac{1}{\sqrt{5}} \right)$$

结式的应用：参数曲线的隐式化

椭圆的参数方程

$$x = \frac{t}{t^2 + 1}, \quad y = \frac{2}{t^2 + 1},$$

其中 t 为参数. 计算椭圆关于 x 和 y 的**隐式方程** (\Rightarrow 消去参数 t)

- ① 引入多项式 $P_1 = (t^2 + 1)x - t, P_2 = (t^2 + 1)y - 2$
- ② 计算 P_1 与 P_2 关于 t 的结式

$$R = \text{res}(P_1, P_2, t) = 4x^2 + y^2 - 2y$$

- ③ $R = 0$ 即为所求的椭圆隐式方程 (Why?)

课后编程练习

1. 编写程序计算环上两个一元多项式关于某个变元的 Sylvester 结式: 输入为 $F, G \in \mathcal{R}[x]$ 和 x , 输出为 $\text{res}(F, G, x)$.

- 可以利用下式验证结果

$$\text{res}((t^2 + 1)x - t, (t^2 + 1)y - 2, t) = 4x^2 + y^2 - 2y$$

2. 利用上述程序解决如下曲面的隐式化问题, 即计算满足下述参数方程的仅含 x, y, z 的隐式多项式.

$$x = \frac{t^3}{2}, \quad y = \frac{(s^2 - 1)t^2}{s^2 + 1}, \quad z = \frac{2st^2}{s^2 + 1}$$

几点提示

- ① 建议用 Maple 软件写, 因为已经有常见的处理矩阵和多项式的函数 ([和计算结式的函数 `resultant\(F, G, x\)`...](#))
- ② 利用 Maple 编写程序时可能需要用到的函数
 - `degree(F, x)`: 返回多项式 F 关于变元 x 的次数
 - `coeff(F, x, n)`: 返回多项式 F 关于 x^n 的系数
 - `Matrix(n)`: 构造一个 $n \times n$ 的全零矩阵
 - `factor(F)`: 返回多项式 F 的因式分解
 - 矩阵赋值可以在[帮助文件](#)中搜索 `Matrix Assignment`
 - `LinearAlgebra[Determinant](M)`: 返回矩阵 M 的行列式
 - 基本 `for` 循环等命令自己查帮助文件
- ③ 第 2 问需要消去两个变元 s 和 t , 但是结式一次只能消去一个变元, [因此...](#)
- ④ 源程序应包含[适量的注释](#)

Gröbner 基

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 $F_1, \dots, F_r \in \mathcal{K}[\boldsymbol{x}]$, 则由 F_1, \dots, F_r 生成的理想为

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

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 $\langle F_1, \dots, F_r \rangle$
- 关于多项式理想的**基础问题**
- VS 线性空间成员判定问题: $v \in b_1, \dots, b_s$ 生成的线性空间?

多项式：从项的角度，项序

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

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

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

常见的全序

设 $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $\mathbf{x}^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathfrak{T}(\mathbf{x})$

- ① **字典序 (lexicographical order):** $\mathbf{x}^\alpha <_{\text{lex}} \mathbf{x}^\beta \Leftrightarrow$
存在 i ($1 \leq i \leq n$), $\alpha_j = \beta_j$ ($i+1 \leq j \leq n$) 且 $\alpha_i < \beta_i$
- ② **分次逆字典序 (graded reverse lexicographical order):**
 $\mathbf{x}^\alpha <_{\text{grevlex}} \mathbf{x}^\beta \Leftrightarrow$
 $\text{tdeg}(\mathbf{x}^\alpha) < \text{tdeg}(\mathbf{x}^\beta)$, 或者 $\text{tdeg}(\mathbf{x}^\alpha) = \text{tdeg}(\mathbf{x}^\beta)$ 且 $\mathbf{x}^\alpha <_{\text{rlex}} \mathbf{x}^\beta$.

项序

Example

设变元序为 $x < y < z$. 多项式

$$x^2yz + 2x^3yz + 3xy^3 + 4y^2z^2 \in \mathbb{Z}[x, y, z]$$

可按字典序、分次字典序和分次逆字典序从大到小排列:

- 字典序: $4y^2z^2 + 2x^3yz + x^2yz + 3xy^3$;
- 分次字典序: $2x^3yz + 4y^2z^2 + x^2yz + 3xy^3$;
- 分次逆字典序: $2x^3yz + 4y^2z^2 + 3xy^3 + x^2yz$.

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

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

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

多项式约化

多项式约化

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

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

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

设 $\mathcal{P} \subseteq \mathcal{K}[\mathbf{x}]$, 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 $\{P_1, \dots, P_r\}$ 的范式是 R 意味着什么?
 $\Rightarrow F - R \in \langle P_1, \dots, P_r \rangle$

Example

对多项式环 $K[x, y]$, 取变元序为 $x < y$, 项序为字典序. 考虑多项式 $F = x^2y^3 + 2xy^2 + x + 1$ 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:

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

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

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

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

为简单起见, 我们将 $<$ 诱导的多项式序 $<'$ 仍记为 $<$.

- 比较项的大小 \implies 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 $([Q_1, \dots, Q_s], R) := \text{PolyRed}([P_1, \dots, P_s], F)$

输入: $[P_1, \dots, P_s] \subseteq \mathcal{K}[\mathbf{x}], F \in \mathcal{K}[\mathbf{x}]$.
输出: $[Q_1, \dots, Q_s] \subseteq \mathcal{K}[\mathbf{x}], R \in \mathcal{K}[\mathbf{x}]$ 满足
 (a) $F = \sum_{i=1}^s Q_i P_i + R$;
 (b) R 模 $\{P_1, \dots, P_s\}$ 已约化;
 (c) 当 $Q_i P_i \neq 0$ 时, $\text{ht}(Q_i P_i) \leq \text{ht}(F)$.

$Q_i := 0$ ($i = 1, \dots, s$), $R := F$;
while R 模 $\{P_1, \dots, P_s\}$ 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 $([Q_1, \dots, Q_s], R)$;

- 终止性

多项式理想成员判定问题

Example

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

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

- 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 $\mathcal{K}[x]$ 中由项集 $\{x^\alpha : \alpha \in S\}$ 生成的理想为**项理想 (term ideal)**, 记作 $\langle x^\alpha : \alpha \in S \rangle$.

- 项理想中的元素并非都是项.

引理

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

命题

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

- $F \in \mathfrak{a}$;
- F 的每一项都在 \mathfrak{a} 中;
- 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

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

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

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

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

Hilbert 基定理 (证明)

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

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 $\mathcal{K}[\mathbf{x}]$ 中理想均存在**有限生成元**. 即对任意 $\mathfrak{a} \subseteq \mathcal{K}[\mathbf{x}]$, 存在 $G_1, \dots, G_s \in \mathfrak{a}$ 使得 $\mathfrak{a} = \langle G_1, \dots, G_s \rangle$.

理想的升链条件 (证明)

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

等价性

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

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

Gröbner 基：定义和存在性

定义

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

$$\langle \text{ht}(G_1), \dots, \text{ht}(G_s) \rangle = \langle \text{ht}(\mathfrak{a}) \rangle,$$

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

范式计算的惟一性 (证明: 反证)

设 $F \in \mathcal{K}[\mathbf{x}]$, 而 $\mathcal{G} = \{G_1, \dots, G_s\}$ 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 $\text{nform}(F, \mathcal{G})$

理想成员的判定问题 (证明)

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

Gröbner 基：消元性质

取 $\mathcal{K}[\mathbf{x}]$ 上的变元序为 $x_1 < \dots < x_n$, 项序为字典序. 对 $1 \leq l \leq n$, 记 $\mathbf{x}_l = (x_1, \dots, x_l)$. 对理想 $\mathfrak{a} \subseteq \mathcal{K}[\mathbf{x}]$, 易证 $\mathfrak{a} \cap \mathcal{K}[\mathbf{x}_l]$ 为 $\mathcal{K}[\mathbf{x}_l]$ 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

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

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

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 $A = F(s, t) - W(s, t)\mathbf{x}$, $B = G(s, t) - W(s, t)\mathbf{y}$, $C = H(s, t) - W(s, t)\mathbf{z}$, 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 :

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

令 $A = st^2\mathbf{x} - (st^2 - t)$, $B = st^2\mathbf{y} - (st + s)$, $C = st^2\mathbf{z} - (2s - 2t)$.
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

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

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 $\text{lcm}(\mu, \nu) = x_1^{m_1} \cdots x_n^{m_n}$, 其中 $m_i = \max(k_i, l_i)$.

定义

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

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

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 $F = 2x^4y - x^2y + 2x$ 与 $G = 4x^3y^2 + y$ 的 S 多项式为

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

Gröbner 基的计算

引理

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

定理: S 对准则

设 $\mathcal{G} = \{G_1, \dots, G_s\}$ 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 $i \neq j$, $S(G_i, G_j)$ 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 $\mathcal{G} := \text{GröbnerBasis}(\mathcal{F})$

输入: $\mathcal{F} = [F_1, \dots, F_s] \subseteq \mathcal{K}[x]$.

输出: \mathcal{F} 的 Gröbner 基 \mathcal{G} , 满足 $\mathcal{F} \subseteq \mathcal{G}$.

$\mathcal{G} := \mathcal{F}$;

$\mathcal{L} := \{\{G_i, G_j\} : G_i, G_j \in \mathcal{G} \text{ 使得 } G_i \neq G_j\}$;

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

$\{G_i, G_j\} := \text{pop}(\mathcal{L})$;

$R := S(G_i, G_j)$ 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

课后编程练习

- ① 设项序为字典序, 编写程序实现多元多项式 $F \in \mathcal{K}[\mathbf{x}]$ 模多元多项式组 $\mathcal{P} \subset \mathcal{K}[\mathbf{x}]$ 的约化算法
- ② 设项序为字典序, 编写程序实现计算多元多项式组 $\mathcal{F} \subset \mathcal{K}[\mathbf{x}]$ 的 Gröbner 基的 Buchberger 算法
- ③ 利用字典序 Groebner 基进行下述有理曲面的隐式化:

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

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** 软件进行编程时的提示
 - **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 $\mathcal{G} := \text{GröbnerBasis}(\mathcal{F})$

输入: $\mathcal{F} = [F_1, \dots, F_s] \subseteq \mathcal{K}[\boldsymbol{x}]$.

输出: \mathcal{F} 的 Gröbner 基 \mathcal{G} , 满足 $\mathcal{F} \subseteq \mathcal{G}$.

$\mathcal{G} := \mathcal{F};$

$\mathcal{L} := \{\{G_i, G_j\} : G_i, G_j \in \mathcal{G} \text{ 使得 } G_i \neq G_j\};$

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

$\{G_i, G_j\} := \text{pop}(\mathcal{L});$

$R := S(G_i, G_j)$ 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: $F \in \langle P_1, \dots, P_r \rangle?$
- 那如何判断两个理想相等呢? $\langle P_1, \dots, P_r \rangle = \langle Q_1, \dots, Q_r \rangle?$

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 $\text{ht}(G) \in \langle \text{ht}(\mathcal{G} \setminus \{G\}) \rangle$, 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 $G \in \mathcal{G}'$, $\text{ht}(G) \notin \langle \text{ht}(\mathcal{G}' \setminus \{G\}) \rangle$.

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

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

→ Buchberger 算法中很多约化均为 0 (Maple 例子)

→ 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 $\text{lcm}(\text{ht}(F), \text{ht}(G)) = \text{ht}(F) \text{ht}(G)$, 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 $Z(\mathcal{F})$ 记 \mathcal{F} 在 \mathcal{K} 的代数闭包 $\bar{\mathcal{K}}$ 中的公共零点构成的集合.

多项式方程组到理想

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

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

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

- 易证 $Z(\mathcal{F}) = Z(\langle \mathcal{F} \rangle) \implies$ 若 $\langle \mathcal{F} \rangle = \langle \mathcal{G} \rangle$, 则 $Z(\mathcal{F}) = Z(\mathcal{G})$.
- 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 \implies 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)

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

设方程组 $\mathcal{F} = 0$ 在 $\bar{\mathcal{K}}$ 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

设 $\mathcal{F} \subseteq \mathcal{K}[\mathbf{x}]$, 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 $1 \leq i \leq n$, 均存在正整数 m_i 与多项式 $G_i \in \mathcal{G}$ 使得 $\text{ht}(G_i) = x_i^{m_i}$.
- 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 $\mathcal{F} = \{x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz - 1\}$. 首先计算 \mathcal{F} 关于 $x < y < z$ 的字典序 Gröbner 基

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

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 $x^4 - 3x^2 + 2 = 0$ 有四个解 $x = \pm 1, \pm \sqrt{2}$. 将其依次代入 $2y^2 + x^2 - 5 = 0$ 与 $2z + x^3 - 3x = 0$ 即可求得全部解

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

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, $\mathcal{G} \cap \mathcal{K}[x_l]$ 正好是理想 $\mathfrak{a} \cap \mathcal{K}[x_l]$ 的 Gröbner 基, 它反映了 \mathfrak{a} 消去变量 x_{l+1}, \dots, x_n 后的结果.

给定 l ($1 \leq l \leq n$), 并设 \mathfrak{a}_l 为 \mathfrak{a} 的第 l 个消去理想. 若 $\mathbf{a} = (a_1, \dots, a_l) \in \mathbb{Z}(\mathfrak{a}_l)$, 则称 \mathbf{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)

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

$$F_i = G_i \mathbf{x}_n^{N_i} + H_i,$$

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

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

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

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 $\mathfrak{a}_1 = \{0\} \Rightarrow$ 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 $x^2 \Rightarrow$ 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 \Rightarrow 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

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 $\mathcal{K}[x_1, \dots, x_n]$: $x_1 < \dots < x_n$

定义

称有限非空有序集合 $[T_1, \dots, T_r] \subseteq \mathcal{K}[x]$ 为**三角列** (triangular set), 如果 $0 < \text{lv}(T_1) < \dots < \text{lv}(T_r)$.

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

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

带余除法算法

算法 2 带余除法 $(Q, R) := \text{Rem}(F, G)$

输入: 多项式 $F, G \in \mathcal{K}[x]$.

输出: F 关于 G 的商 Q 和余式 R .

$Q := 0; R := F; l := \deg(G);$

while $\deg(R) \geq l$ **do**

$r := \deg(R);$

$R := R - (\text{lc}(R)/\text{lc}(G))x^{r-l}G;$

$Q := Q + (\text{lc}(R)/\text{lc}(G))x^{r-l};$

end

return $(Q, R);$

例: $x^3 + 2x + 1$ 除以 $2x + 3 \in \mathbb{Q}[x]$

问: $x^3 + 2x + 1$ 除以 $2x + 3 \in \mathbb{Z}[x]?$

多元多项式的伪除

命题 (伪除, 证明)

设 $F, G \in \mathcal{R}[\mathbf{x}]$, x_k 为一变元, 且 $l = \deg(G, x_k)$, $m = \deg(F, x_k)$.
若 $l > 0$, 则存在 $Q, R \in \mathcal{R}[\mathbf{x}]$ 以及整数 $0 \leq s \leq m - l + 1$ 使得

$$\text{lc}(G, x_k)^s F = QG + R, \quad \text{且 } \deg(R, x_k) < l. \quad (2)$$

若固定 s , 则 Q, R 唯一确定.

- 表达式 (2) 为 F 关于 G 的**伪余公式** (pseudo-remainder formula)
- Q : F 对 G 关于 x_k 的**伪商** (pseudo-quotient), $\text{pquo}(F, G, x_k)$
- R 为 F 对 G 关于 x_k 的**伪余式** (pseudo-remainder), $\text{prem}(F, G, x_k)$
- 称 F 关于 G 是**约化的 (reduced)**: $\deg(F, \text{lv}(G)) < \text{ldeg}(G)$,
显然 $\text{prem}(F, G)$ 关于 G 是约化的

多元多项式的伪除

算法 1 伪除 $(Q, R, s) := \text{Prem}(F, G, x_k)$

输入: 多项式 $F, G \in \mathcal{R}[x]$, 变元 x_k 使得 $\deg(G, x_k) > 0$.

输出: F 对 G 关于 x_k 的伪商 Q 和伪余式 R , 以及整数 s 使得 (1.4) 式成立.

$R := F; Q := 0; l := \deg(G, x_k); s := 0;$

while $\deg(R, x_k) \geq l$ **do**

$r := \deg(R, x_k);$

$R := \text{lc}(G, x_k)R - \text{lc}(R, x_k)x_k^{r-l}G;$

$Q := \text{lc}(G, x_k)Q + \text{lc}(R, x_k)x_k^{r-l};$

$s := s + 1;$

end

return $(Q, R, s);$

Example

考虑多项式 $F = 2y^3 - y^2 + x^2y$, $G = xy^2 + 1$. 由伪除算法可得 F 对 G 关于 y 的伪余公式为

$$\textcolor{red}{x}^2 F = (2\textcolor{red}{x}y - \textcolor{red}{x})G + \textcolor{red}{x}^4 y - 2\textcolor{red}{x}y + \textcolor{red}{x}.$$

特别有,

$$\text{pquo}(F, G, y) = 2xy - x,$$

$$\text{prem}(F, G, y) = x^4 y - 2xy + x.$$

对三角列的伪除

多项式组的零点

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

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

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

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

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

且伪除关系如下 (推导)

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

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

对三角列的伪除

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

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

设 $\mathcal{T} \subseteq \mathcal{K}[\mathbf{x}]$ 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.

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

引理 (证明)

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

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

特征列

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

特征列

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

定理: (证明, 特征列的零点关系)

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

$$\mathcal{Z}(\mathcal{C}/\mathcal{I}) \subseteq \mathcal{Z}(\mathcal{P}) \subseteq \mathcal{Z}(\mathcal{C}), \quad (3)$$

$$\mathcal{Z}(\mathcal{C}/\mathcal{I}) = \mathcal{Z}(\mathcal{P}/\mathcal{I}), \quad (4)$$

$$\mathcal{Z}(\mathcal{P}) = \mathcal{Z}(\mathcal{C}/\mathcal{I}) \cup \bigcup_{i=1}^r \mathcal{Z}(\mathcal{P}_i). \quad (5)$$

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。

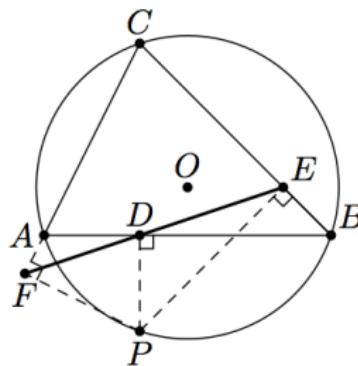


图 6.2 Simson 定理

(只证 \Leftarrow)

几何定理机器证明

将几何问题转换为代数问题 \Rightarrow 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:

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

假设条件：

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

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



满足定理假设条件的任意点，均满足定理结论



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

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

已知关于特征列零点的结论

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

几何定理机器证明：示例

计算得到特征列如下

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

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 $\pm i$);
- (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

问题可以归结为判定包含关系 $Z(\mathcal{H}) \subseteq Z(G)$ 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 $Z(\mathcal{H}) \subseteq Z(G)$ 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 $x_1 < \dots < x_n$ 的特征列, 而 $I = \prod_{C \in \mathcal{C}} \text{ini}(C)$. 若 $\text{prem}(G, \mathcal{C}) \equiv 0$, 则 $Z(\mathcal{H}/I) \subseteq Z(G)$, 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 $\text{prem}(F, \mathcal{C}) \neq 0$ 怎么办?

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

吴特征列算法：秩

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

多项式的秩

设 $P, Q \in \mathcal{K}[\mathbf{x}]$ 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 $\text{cls}(P) < \text{cls}(Q)$; (类大的大于类小的)
- ③ $P, Q \notin \mathcal{K}$, $\text{cls}(P) = \text{cls}(Q)$, 且 $\text{ldeg}(P) < \text{ldeg}(Q)$. (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 $\mathcal{T} = [T_1, \dots, T_r]$ 和 $\mathcal{S} = [S_1, \dots, S_t]$ 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 $i \leq \min(r, t)$, 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 $j \leq t$ 都有 $T_j \sim S_j$ 成立.

定义：基列

对任意非空有限多项式集合 $\mathcal{P} \subseteq \mathcal{K}[\mathbf{x}]$, 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 $\mathcal{B}_1 \sim \mathcal{B}_2$
- 对任意多项式组 \mathcal{P} , 容易构造它的一个基列

吴特征列算法：特征列的计算

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

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

输出: \mathcal{P} 的特征列 \mathcal{C} .

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

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

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

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

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

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

end

return $\mathcal{C};$

- **VS** Buchberger 算法?

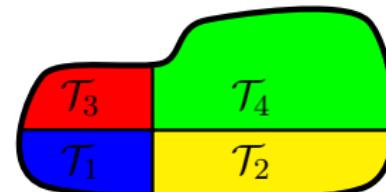
三角分解

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



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

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



三角分解

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

特征分解

定理 (特征列的零点关系)

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

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

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

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

- $\mathcal{C} \subseteq \langle \mathcal{P} \rangle \subseteq \langle \mathcal{P}_i \rangle \implies \mathsf{Z}(\mathcal{P}_i) \subseteq \mathsf{Z}(\mathcal{C}) \implies \mathsf{Z}(\mathcal{P}_i \cup \mathcal{C}) = \mathsf{Z}(\mathcal{P}_i)$
- 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

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

↓

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

$$\mathcal{T}_2 = [\textcolor{blue}{x_1 - 2}, \textcolor{blue}{x_2 + 8}, \textcolor{blue}{6x_3^3 + 8x_3^2 + 13}]$$

$$\mathcal{T}_3 = [x_1 + 1, x_2 - 1, x_3^2 + 2]$$

- \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

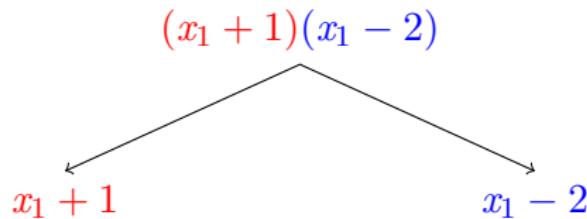
不可约分解：示例

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

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

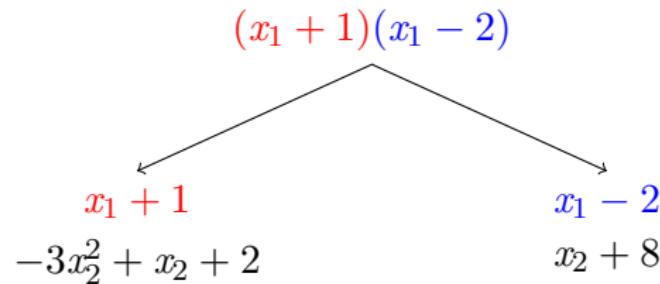
不可约分解：示例

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



不可约分解：示例

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



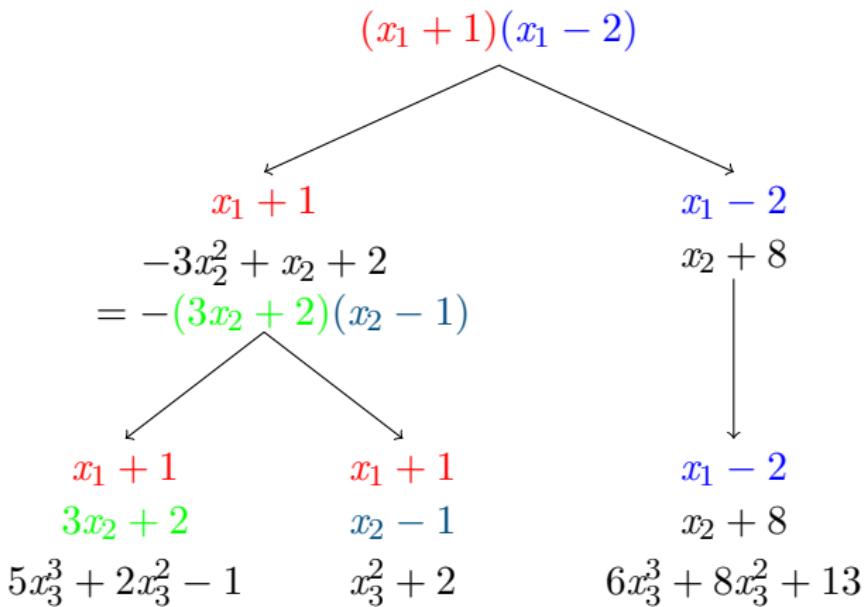
不可约分解：示例

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

$$\begin{array}{c} (x_1 + 1)(x_1 - 2) \\ \swarrow \qquad \searrow \\ x_1 + 1 \qquad \qquad \qquad x_1 - 2 \\ -3x_2^2 + x_2 + 2 \qquad \qquad \qquad x_2 + 8 \\ = -(3x_2 + 2)(x_2 - 1) \end{array}$$

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、 $Z(\mathcal{T}/\text{ini}(\mathcal{T})) \neq \emptyset$.

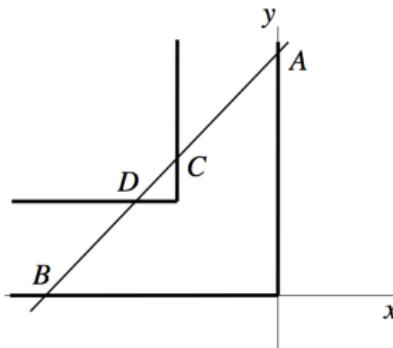
设 $\mathcal{T} = [T_1, \dots, T_r] \subset \mathcal{K}[\boldsymbol{x}]$ 为三角列

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

柱形代数分解

搬钢琴问题

问题：确定一把长度为 3、充分细的梯子能否穿过宽度为 1 的直角走廊的拐角



● 机器人运动规划

走廊可以用下述集合表示

$$\left\{ (x, y) \in \mathbf{R}^2 \mid x \leq 0, 0 \leq y \leq 1 \right\} \cup \left\{ (x, y) \in \mathbf{R}^2 \mid y \geq 0, -1 \leq x \leq 0 \right\}$$

搬钢琴问题

容易发现，梯子不能穿过走廊的拐角**当且仅当**梯子与四面墙
 $\{x = 0, y \geq 0\}, \{y = 0, x < 0\}, \{x = -1, y \geq 1\}, \{y = 1, x < -1\}$
 均相交.

- 设梯子与四面墙的交点为 $A(0, a), B(b, 0), C(-1, c), D(d, 1)$ ，
 则相应的**约束条件**为：

$$\left\{ \begin{array}{ll} a \geq 0, b < 0, c \geq 1, d < -1, & (A, B, C, D \text{ 分别位于四面墙上}) \\ a^2 + b^2 \leq 9, & (|AB| \leq 3 = \text{梯子的长度}) \\ d - (1 - a)(d - b) = 0, & (A, D, B \text{ 三点共线}) \\ c - (1 + b)(c - a) = 0. & (A, C, B \text{ 三点共线}) \end{array} \right.$$

- 梯子无法通过等价于 (取**实数值**)

$$(\exists a, b, c, d) [a \geq 0 \wedge b < 0 \wedge c \geq 1 \wedge d < -1 \wedge a^2 + b^2 \leq 9 \wedge \\ d - (1 - a)(d - b) = 0 \wedge c - (1 + b)(c - a) = 0].$$

量词消去的基本概念

如何将带量词的公式转化为等价的无量词公式：量词消去

高中！ $\exists x \ ax^2 + bx + c = 0 \Leftrightarrow b^2 - 4ac \geq 0$

基本定义

- **变量**: 形如 x, y, z 的符号; **代数常量**: 整数; **代数运算符**: 指 $+, -, \cdot$ 和 \cdot
- **代数项**: 由变量和代数常量通过代数运算符号连接得到的**有意义的表达式**
- **二元关系运算符**: $=, \neq, >, <, \leq$ 和 \geq
- **原子公式**: 形如 $P \sim 0$ 的表达式, 其中 P 为代数项, \sim 表示某个二元关系运算符
- **逻辑联结词**: 包含 \vee (或), \wedge (且) 和 \neg (非);
- **Tarski 公式**: 通过逻辑联结词和量词 (\exists, \forall) 将原子公式连接而成的表达式.
- $\rightarrow, \leftrightarrow$: $A \rightarrow B := A \wedge \neg B, A \leftrightarrow B := A \rightarrow B \wedge B \rightarrow A$

量词消去的基本概念

示例

- $x, x + y, (x + y) \cdot z$ 都是代数项
- $x+, x + \sqrt{3}$ 不是代数项, 因为 $x+$ 是无意义的表达式, $x + \sqrt{3}$ 含有非法符号 $\sqrt{3}$.
- 原子公式:
 - $0 = 0$
 - $1 + 1 \neq 0$
 - $x^2 + y - x > 0$
 - $x^3 + x < 0$
 - $x + xy + y^2 \leq 0$
- Tarski 公式:
 - $0 = 0$
 - $(\exists x)[x^2 - 1 = 0]$
 - $(x = 0) \vee (\exists y)[x - y = 0]$
 - $(\exists x)\neg(\exists y)\neg[(x - y = 0) \wedge (x - (1 + y) > 0)]$
 - $\neg(x - 1 > 0) \wedge (\exists y)[x - y^2 = 0]$

量词消去的定义

无量词公式

称不含量词的 Tarski 公式为 **无量词公式 (quantifier-free formula)**.

- 例如 $(x > 0) \wedge (x^2 - 2 = 0)$ 为无量词公式, 它定义了 \mathbb{R} 中的无理数 $\sqrt{2}$.

量词消去

给定一含量词 (\forall, \exists) 的 Tarski 公式, 求一个与之等价的无量词公式.

- 例如, 对 $(\forall x)[ax^2 + bx + c > 0]$ 约化可得到等价的无量词公式

量词消去的定义

无量词公式

称不含量词的 Tarski 公式为 **无量词公式 (quantifier-free formula)**.

- 例如 $(x > 0) \wedge (x^2 - 2 = 0)$ 为无量词公式, 它定义了 \mathbb{R} 中的无理数 $\sqrt{2}$.

量词消去

给定一含量词 (\forall, \exists) 的 Tarski 公式, 求一个与之等价的无量词公式.

- 例如, 对 $(\forall x)[ax^2 + bx + c > 0]$ 约化可得到等价的无量词公式 $(a > 0) \wedge (b^2 - 4ac < 0)$.

问题: 是否量词消去总能进行?

Taski 定理

定理

设 $\Phi = (\exists_k x)[\Phi_1 \wedge \dots \wedge \Phi_r]$, 其中 Φ_i 形如 $F = 0$ 或 $F > 0$, 则存在有效算法来计算与 Φ 等价的无量词公式.

不含自由变量的 Tarski 公式称为 Tarski 命题或初等代数命题.

- 例: $(\forall a)[a^2 - 2a < 0]$ 或 $a \neq 0 \rightarrow ax + b = 0$ 有一根
- 初等代数命题均可判断真假

Tarski 定理

设 Φ 为初等代数命题, 则存在有效的判定算法来判定 Φ 的真假.

- 量词使得命题真假难以确定 \Rightarrow 量词消去 \Rightarrow 可以判定
- 实几何中初等问题的可判定性: Hilbert, Gödel, Tarski
- 构造性方法, 但复杂度太高

柱形代数分解



George E. Collins (1928–2017)

He is the inventor of garbage collection by [reference counting](#) and of the method of quantifier elimination by [cylindrical algebraic decomposition](#).

半代数集

半代数集

设 $S \subseteq \mathbb{R}^n$. 若 S 可由

$$\bigcup_{i=1}^s \bigcap_{j=1}^{t_i} \{ \mathbf{a} \in \mathbb{R}^n : F_{ij}(\mathbf{a}) \sim 0 \}$$

表示, 其中 $F_{ij} \in \mathbb{R}[\mathbf{x}]$, $\sim \in \{=, >, <, \geq, \leq, \neq\}$, 则称 S 为 \mathbb{R}^n 中的半代数集 (semi-algebraic set), 并将 $\{F_{ij} : 1 \leq i \leq s, 1 \leq j \leq t_i\}$ 称为 S 的定义多项式组.



半代数集的基本性质

半代数集的基本性质

- ① 设 $P \in \mathbb{R}[\mathbf{x}]$, 则 $\{\mathbf{a} \in \mathbb{R}^n : P(\mathbf{a}) = 0\}$ 和 $\{\mathbf{a} \in \mathbb{R}^n : P(\mathbf{a}) > 0\}$ 是半代数集.
- ② 设 S_1, S_2 为半代数集, 则 $S_1 \cap S_2$, $S_1 \cup S_2$ 及 $\mathbb{R}^n \setminus S_1$ 也是半代数集. (交、并、补)
- ③ 设 S_1 和 S_2 分别为 \mathbb{R}^n 和 \mathbb{R}^m 中的半代数集, 则 $S_1 \times S_2$ 是 $\mathbb{R}^n \times \mathbb{R}^m$ 中的半代数集.(笛卡尔积)

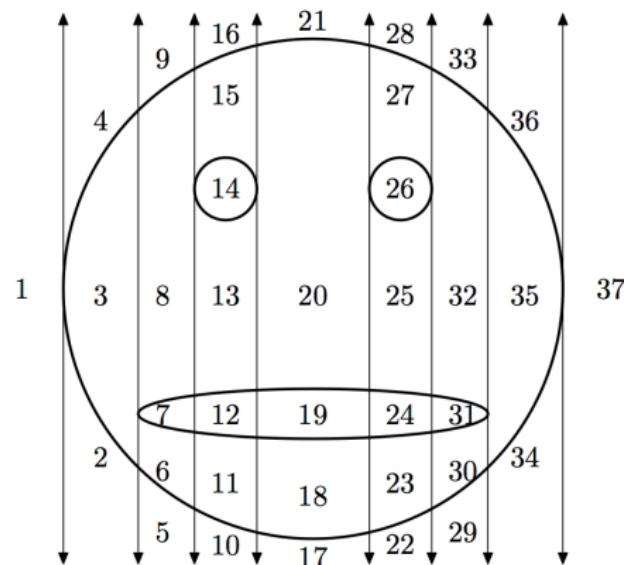
示例

- ① \mathbb{R} 中的半代数集是有限个点和开区间的并.
- ② 设 S 为 \mathbb{R}^n 中的半代数集, σ 为 \mathbb{R}^n 到 \mathbb{R}^s 的映射, 并且 $\sigma(\mathbf{x}) = (F_1, \dots, F_s)$, $F_i \in \mathbb{R}[\mathbf{x}]$ ($1 \leq i \leq s$), 则 $\sigma(S)$ 也为半代数集.

柱形代数分解: 大意

设 $\mathcal{F} = \{F_1, \dots, F_s\} \subseteq \mathbb{R}[\boldsymbol{x}]$, 利用 \mathcal{F} 对 \mathbb{R}^n 进行柱形代数分解就是要从 \mathcal{F} 构造出一个 \mathbb{R}^n 的有限胞腔分解, 并且在每个胞腔上 \mathcal{F} 中所有多项式的符号恒定。

- 验证符号只需在每个胞腔中取样本点



柱形代数分解：步骤

Tarski–Seidenberg 定理

将 \mathbb{R}^n 中的半代数集投影到 \mathbb{R}^{n-1} 上仍得到半代数集.

计算 \mathbb{R}^n 的一个 \mathcal{F} 的柱形代数分解及其样本的步骤.

- ① **投影**: 将一个半代数集通过连续的投影得到新的半代数集, 在投影的过程中半代数集的维数依次递减. 设初始半代数集是在 \mathbb{R}^n 中定义的, 则依次投影直至得到 \mathbb{R} 上的一元多项式.
- ② **一元情形**: 投影完成后, 利用对投影得到的一元多项式的根来分解 \mathbb{R} , 从而得到包含**一维胞腔** (区间) 和**零维胞腔** (孤立点) 的 \mathbb{R} 的分解.
- ③ **提升**: 此后, 可以逐次将 \mathbb{R}^r 的胞腔分解提升为 \mathbb{R}^{r+1} 的胞腔分解, 直到提升至 \mathbb{R}^n 为止.
- ④ **测试点**: 在每个胞腔上选取一个**样本点**检验命题成立与否.

柱形代数分解：胞腔

定义：胞腔

称 \mathbb{R} 中的一个开区间或某一点为一维胞腔 (1-dimensional cell).

设 $S \subseteq \mathbb{R}^{n-1}$ 为 $n-1$ 维胞腔，则称形如

$$\{(\bar{x}, y) : \bar{x} \in S, y = f(\bar{x})\} \quad \text{或} \quad \{(\bar{x}, y) : \bar{x} \in S, f(\bar{x}) < y < g(\bar{x})\}$$

的集合为 n 维胞腔 (n -dimensional cell), 其中 f, g 为 $\pm\infty$ 或使得 $f(\bar{x}) < g(\bar{x})$ ($\forall \bar{x} \in S$) 成立的连续实值函数.

- 若存在 $F, G \in \mathbb{R}[\mathbf{x}, y]$ 使得 $F(\mathbf{x}, f(\mathbf{x})) = 0, G(\mathbf{x}, g(\mathbf{x})) = 0$, 则称如上定义的胞腔为代数胞腔 (algebraic cell).

代数叠加

设 $n-1$ 维区域 S 上有连续实值函数 $-\infty = f_0 < f_1 < \dots < f_l < f_{l+1} = +\infty$, 并且对任意 i ($1 \leq i \leq l$) 都存在 $F_i \in \mathbb{R}[\mathbf{x}, y]$ 使得 $F(\mathbf{x}, f_i(\mathbf{x})) = 0$, 则由 f_i 和 (f_i, f_{i+1}) ($0 \leq i \leq l$) 可以确定柱形 $Z(S)$ 的一个代数分解, 称该分解为 S 上的一个由 f_1, \dots, f_l 定义的代数叠加.

柱形代数分解：定义

\mathbb{R}^n 的柱形代数分解 (cylindrical algebraic decomposition) 可以递归定义如下：

① 当 $n = 1$ 时, \mathbb{R} 可分解为有限个实代数数, 设为 $a_1 < \dots < a_t$ 以及由这些实代数数界定的有界和无界的开区间, 则所得
到的柱形代数分解为

$$((-\infty, a_1), [a_1, a_1], \dots, (a_{i-1}, a_i), [a_i, a_i], (a_i, a_{i+1}), \dots, [a_t, a_t], (a_t, +\infty)).$$

② 当 $n > 1$ 时, 存在 \mathbb{R}^{n-1} 的一个柱形代数分解 $\mathcal{C}_{n-1} = (S_1, \dots, S_l)$ 使得

$$\mathcal{C}_n = (S_{1,1}, \dots, S_{1,2m_1+1}, \dots, S_{l,1}, \dots, S_{l,2m_l+1}),$$

这里, 对任意 i ($1 \leq i \leq l$), $(S_{i,1}, \dots, S_{i,2m_i+1})$ 都是 S_i 上的一个代数叠加. 此时, \mathcal{C}_{n-1} 称为 \mathcal{C}_n 诱导的 \mathbb{R}^{n-1} 上的柱形代数分解.

柱形代数分解: $n = 1$

设 \mathbb{R} 中的半代数集 S 由 $\mathcal{F} = \{F_i \in \mathbb{R}[x] : 1 \leq i \leq s\}$ 定义.
 令 $F = \prod_{i=1}^s F_i$, 又设 F 的互异实根为 a_1, \dots, a_t , 并且

$$a_1 < \cdots < a_{i-1} < a_i < a_{i+1} < \cdots < a_t.$$

于是, \mathbb{R} 的柱形代数分解为

$$((-\infty, a_1), [a_1, a_1], \dots, (a_{i-1}, a_i), [a_i, a_i], (a_i, a_{i+1}), \dots, [a_t, a_t], (a_t, +\infty)).$$

对应样本点的选取方法为:

- ① $(-\infty, a_1)$ 和 $(a_t, +\infty)$ 的样本点分别取为 $a_1 - 1$ 和 $a_t + 1$
- ② 对于有限长度的一维胞腔 (a_i, a_{i+1}) , 样本点取为区间中点
- ③ 零维胞腔 $[a_i, a_i]$, 样本点即为 a_i .

柱形代数分解：投影

以 \mathbb{R}^2 向 \mathbb{R} 的投影为例：

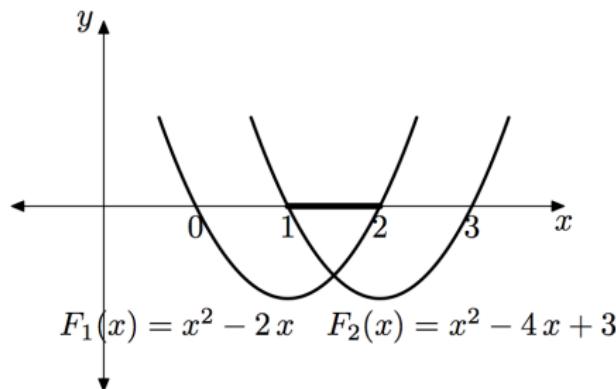
投影算子

设 $\mathcal{F} = \{F_1, \dots, F_s\} \subseteq \mathbb{R}[x, y]$, F_i ($1 \leq i \leq s$) 无平方且两两互素.
定义 \mathcal{F} 的投影算子 (projection operator) 为

$$\begin{aligned}\text{proj}(\mathcal{F}) := & \{\text{lc}(F_i, y) : 1 \leq i \leq s\} \cup \\ & \{\text{disc}(F_i, y) : 1 \leq i \leq s\} \cup \\ & \{\text{res}(F_i, F_j, y) : 1 \leq i < j \leq s\}.\end{aligned}$$

- $\text{lc}(F_i, y)$: F_i 关于 y 的首项系数
- $\text{disc}(F_i, y)$: F_i 关于 y 的判别式 (一元二次方程判别式的推广)
- $\text{res}(F_i, F_j, y)$: F_i 和 F_j 关于 y 的结式

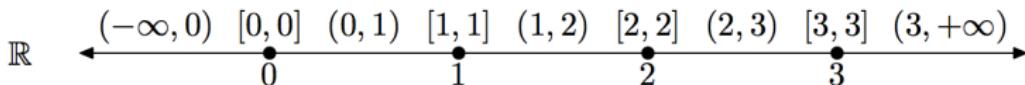
投影算子可以保证由 \mathbb{R}^n 到 \mathbb{R}^{n-1} 的合理映射: 可提升!

柱形代数分解: $n = 1$ 

对于 $F_1 = x^2 - 2x$, $F_2 = x^2 - 4x + 3$, 一维数轴 \mathbb{R} 实施柱形代数分解可得到 5 个一维胞腔和 4 个零维胞腔, 分别为

$$(-\infty, 0), [0, 0], (0, 1), [1, 1], (1, 2), [2, 2], (2, 3), [3, 3], (3, +\infty),$$

对应的样本点可选为 $-1, 0, 1/2, 1, 3/2, 2, 5/2, 3, 4$.



柱形代数分解：提升

已有 \mathbb{R}^{r-1} 的柱形代数分解为 $\mathcal{C}_{r-1} = (S_1, \dots, S_m)$. 对 \mathcal{C}_{r-1} 中的任意 k 维胞腔 S_i , 都可构造 $k+1$ 维集合 $\{(\mathbf{p}, x_r) \in \mathbb{R}^r : \mathbf{p} \in S_i\}$, 其中 $\mathbf{p} = (\bar{x}_1, \dots, \bar{x}_{r-1}) \in \mathbb{R}^{r-1}$.

\mathbb{R}^r 的柱形代数分解 \mathcal{C}_r 的构造过程

对任意 $F \in \mathcal{F}_r$, 令 f_j 为使得 $F(\mathbf{p}, f_j(\mathbf{p})) = 0$ ($1 \leq j \leq m_i$, $m_i = \#\mathcal{F}_r$) 成立的连续实值函数, 并且对任意 $\mathbf{p} \in S_i$ 都有 $f_j(\mathbf{p}) < f_{j+1}(\mathbf{p})$ 成立, 则 \mathbb{R}^r 上的柱形代数分解 \mathcal{C}_r 可定义为 $(S_{1,1}, \dots, S_{1,2r_1+1}, \dots, S_{m,1}, \dots, S_{m,2r_m+1})$, 其中

$$S_{i,1} = \{(\mathbf{p}, x_r) \in \mathbb{R}^r : \mathbf{p} \in S_i, x_r < f_1(\mathbf{p})\},$$

$$S_{i,2j} = \{(\mathbf{p}, x_r) \in \mathbb{R}^r : \mathbf{p} \in S_i, x_r = f_j(\mathbf{p})\} \quad (1 \leq j \leq r_i),$$

$$S_{i,2j+1} = \{(\mathbf{p}, x_r) \in \mathbb{R}^r : \mathbf{p} \in S_i, f_j(\mathbf{p}) < x_r < f_{j+1}(\mathbf{p})\} \quad (1 \leq j < r_i),$$

$$S_{i,2r_i+1} = \{(\mathbf{p}, x_r) \in \mathbb{R}^r : \mathbf{p} \in S_i, f_{r_i}(\mathbf{p}) < x_r\}.$$

柱形代数分解：样本点

设 \mathbb{R}^{r-1} 的柱形分解的样本为 $S'_{\text{sp}} = (\mathbf{s}_1, \dots, \mathbf{s}_m)$, 则 \mathbb{R}^r 的柱形分解样本

$$S_{\text{sp}} = (\mathbf{s}_{1,1}, \dots, \mathbf{s}_{1,2r_1+1}, \dots, \mathbf{s}_{m,1}, \dots, \mathbf{s}_{m,2r_m+1})$$

可以通过下列步骤构造:

- ① $\mathbf{s}_{i,j}$ 的前 $r - 1$ 个坐标取 \mathbf{s}_i 的相应坐标;
- ② $\mathbf{s}_{i,1}$ 的第 r 个坐标可取为 $f_1(\mathbf{s}_i) - 1$;
- ③ $\mathbf{s}_{i,2j}$ 的第 r 个坐标可取为 $f_j(\mathbf{s}_i)$ ($1 \leq j \leq r_i$);
- ④ $\mathbf{s}_{i,2j+1}$ 的第 r 个坐标可取为 $\frac{1}{2}(f_j(\mathbf{s}_i) + f_{j+1}(\mathbf{s}_i))$ ($1 \leq j < r_i$);
- ⑤ $\mathbf{s}_{i,2r_i+1}$ 的第 r 个坐标可取为 $f_{r_i}(\mathbf{s}_i) + 1$.

柱形代数分解：示例

令 $\mathcal{F} = \{x^2 + y^2 - 1\}$. 对 \mathcal{F} 进行连续投影可以得到 $\mathcal{F}_2 = \{F_2\}$, $\mathcal{F}_1 = \{F_1\}$, 其中 $F_2 = x^2 + y^2 - 1$, $F_1 = x^2 - 1$. 通过计算可得 F_1 的实根为 $-1, 1$, 所以 \mathbb{R} 的 \mathcal{F} 不变号的分解为 $\mathcal{C}_1 = (S_1, \dots, S_5)$, 这里

$$\begin{aligned} S_1 &= [-2, F_1 > 0], & S_2 &= [-1, F_1 = 0], & S_3 &= [0, F_1 < 0], \\ S_4 &= [1, F_1 = 0], & S_5 &= [2, F_1 > 0]. \end{aligned}$$

下面以 S_1 , S_2 和 S_3 为例来说明如何将 \mathcal{C}_1 提升为 \mathbb{R}^2 上的柱形分解. 将 $x = -2$ 代入 F_2 可知 F_2 无实根, 因此将 S_1 提升后对应的柱形分解为 $[(-2, 0), F_1 > 0 \wedge F_2 > 0]$. 将 $x = -1$ 代入 F_2 得到 S_2 提升后对应的柱形分解为

$$([(-1, -1), F_1 = 0 \wedge F_2 > 0], [(-1, 0), F_1 = 0 \wedge F_2 = 0], [(-1, 1), F_1 = 0 \wedge F_2 > 0]).$$

柱形代数分解：示例

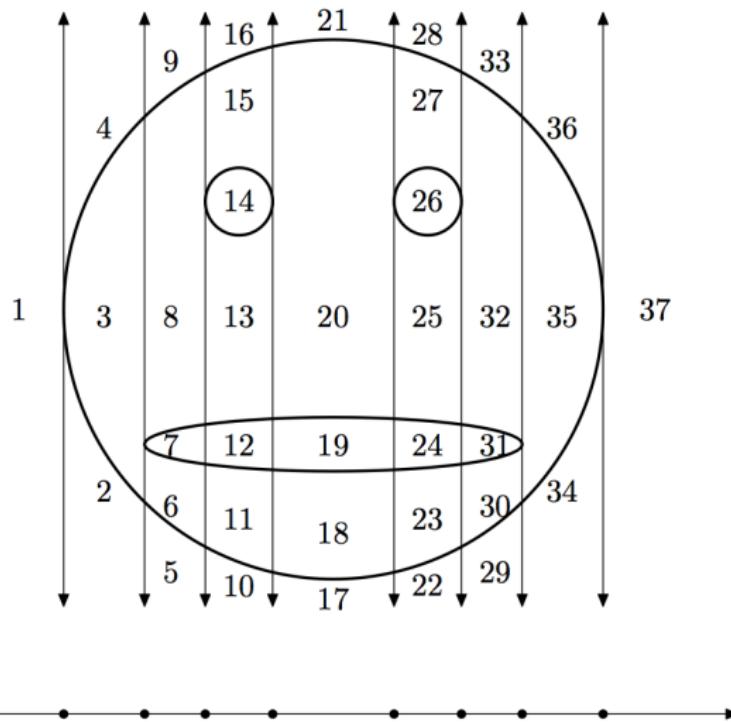
将 $x = 0$ 代入 F_2 并求得其实根为 $-1, 1$. 于是可得 S_3 提升后的柱形分解为

$$\begin{aligned} & [(0, -2), F_1 < 0 \wedge F_2 > 0], [(0, -1), F_1 < 0 \wedge F_2 = 0], \\ & [(0, 0), F_1 < 0 \wedge F_2 < 0], [(0, 1), F_1 < 0 \wedge F_2 = 0], \\ & [(0, 2), F_1 < 0 \wedge F_2 > 0]). \end{aligned}$$

类似地得到 S_4 和 S_5 的提升, 于是可得 \mathbb{R}^2 的一个柱形代数分解为

$$\begin{aligned} S_{1,1} &= [(-2, 0), F_1 > 0 \wedge F_2 > 0], S_{2,1} = [(-1, -1), F_1 = 0 \wedge F_2 > 0], \\ S_{2,2} &= [(-1, 0), F_1 = 0 \wedge F_2 = 0], S_{2,3} = [(-1, 1), F_1 = 0 \wedge F_2 > 0], \\ S_{3,1} &= [(0, -2), F_1 < 0 \wedge F_2 > 0], S_{3,2} = [(0, -1), F_1 < 0 \wedge F_2 = 0], \\ S_{3,3} &= [(0, 0), F_1 < 0 \wedge F_2 < 0], S_{3,4} = [(0, 1), F_1 < 0 \wedge F_2 = 0], \\ S_{3,5} &= [(0, 2), F_1 < 0 \wedge F_2 > 0], S_{4,1} = [(1, -1), F_1 = 0 \wedge F_2 > 0], \\ S_{4,2} &= [(1, 0), F_1 = 0 \wedge F_2 = 0], S_{4,3} = [(1, 1), F_1 = 0 \wedge F_2 > 0], \\ S_{5,1} &= [(2, 0), F_1 > 0 \wedge F_2 > 0]). \end{aligned}$$

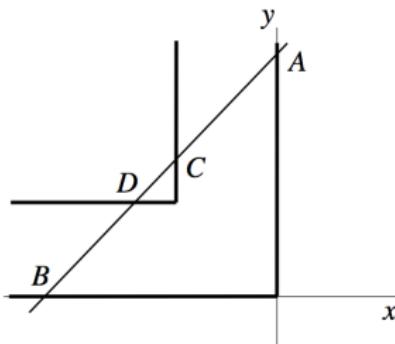
柱形代数分解：示例



- 37 个 2 维胞腔, 64 个一维细胞腔和 28 个零维细胞腔

搬梯子问题

问题：长度为 3 的梯子能否穿过宽度为 1 的直角走廊的拐角



$$(\exists a, b, c, d) [a \geq 0 \wedge b < 0 \wedge c \geq 1 \wedge d < -1 \wedge a^2 + b^2 \leq 9 \wedge d - (1 - a)(d - b) = 0 \wedge c - (1 + b)(c - a) = 0].$$

- 柱形代数分解方法: 不能通过拐角
- 进一步假设梯子的长度 r 未知, 则可以得到类似的梯子无法通过的公式, 利用柱形代数分解可以得到:

$$r^2 > 8 \wedge r > 2.$$

即梯子能通过当且仅当 $r \leq 2\sqrt{2}$.

柱形代数分解：一元方程的解？

柱形代数分解: $n = 1$

设 \mathbb{R} 中的半代数集 S 由 $\mathcal{F} = \{F_i \in \mathbb{R}[x] : 1 \leq i \leq s\}$ 定义.
令 $F = \prod_{i=1}^s F_i$, 又设 F 的互异实根为 a_1, \dots, a_t , 并且

$$a_1 < \cdots < a_{i-1} < a_i < a_{i+1} < \cdots < a_t.$$

于是, \mathbb{R} 的柱形代数分解为

$$((-\infty, a_1), [a_1, a_1], \dots, (a_{i-1}, a_i), [a_i, a_i], (a_i, a_{i+1}), \dots, [a_t, a_t], (a_t, +\infty)).$$

- 如何无误差地计算一元多项式的互异实根?

数值算法的一些问题

- $F(x) = (x+1)(x+2) \cdots (x+20)$: 20个实根, $F(x) - 10^{-9}x^{19}$ 却只有14个实根
- The zero problem: 例如 $\sqrt{2} + \sqrt{3} - \sqrt{5 + 2\sqrt{6}} = 0$?
- $F(x) = 0$?

实根隔离

求 \mathbb{R} 上一列互不相交的有理区间使其包含给定多项式的所有实根, 并且每个区间恰含一个根 (重根看作一个).

算法 31 实根隔离 $L := \text{Realsol}(F)$

输入: 无平方多项式 $F \in \mathbb{R}[x]$, $\deg(F) = m$.

输出: F 的实根隔离区间列 L .

```

 $\mathcal{S} := F$  的 Sturm 序列;
 $b := F$  根的界;  $a := -b$ ;
 $N := \text{var}(\mathcal{S}, a) - \text{var}(\mathcal{S}, b)$ ;
if  $N = 0$  then return  $\emptyset$ ;
 $i := 1$ ;  $L := \emptyset$ ;
 $a_i := a$ ;  $b_i := b$ ;
while  $i \leq N$  do
    while  $\text{var}(\mathcal{S}, a_i) - \text{var}(\mathcal{S}, b_i) > 1$  do
         $c := (a_i + b_i)/2$ ;
        if  $\text{var}(\mathcal{S}, a_i) - \text{var}(\mathcal{S}, c) \geq 1$  then
             $b_i := c$ ;
        else
             $a_i := c$ ;
        end
    end
     $L := L \cup \{[a_i, b_i]\}$ ;
     $i := i + 1$ ;
     $a_i := b_{i-1}$ ;  $b_i := b$ ;
end
return  $L$ ;
```

实根隔离算法

一元实系数多项式根的界

给定 $F \in \mathbb{R}[x]$, 首先需要找到包含 F 所有实根的区间, 即找到 $M > 0$, 使得 F 的所有实根都在区间 $(-M, M)$ 上.

一元实系数多项式根的界

设 $F = \sum_{i=0}^m c_i x^i \in \mathbb{R}[x]$, 并令

$$M = \max \left\{ 1, \sum_{i=0}^{m-1} \left| \frac{c_i}{c_m} \right| \right\}, \quad N = 1 + \max \left\{ \left| \frac{c_0}{c_m} \right|, \dots, \left| \frac{c_{m-1}}{c_m} \right| \right\},$$

则对任意 $|x| \geq M$ 或 $|x| \geq N$, $|F| > 0$.

- 即 $|x| \geq \min(M, N)$.
- 证明:** 主要利用三角不等式

变号数

序列的变号数

设 \mathbf{a} 为 \mathbb{R} 中的序列, 而 $\mathbf{a}' = [a_1, \dots, a_t]$ 为删除 \mathbf{a} 中所有 0 后得到的新序列, 则 \mathbf{a} 的变号数 $\text{var}(\mathbf{a})$ 定义为集合 $\{a_i a_{i+1} \mid 1 \leq i \leq t-1\}$ 中的负数个数, 即

$$\text{var}(\mathbf{a}) = \sum_{i=1}^{t-1} \frac{1 - \text{sgn}(a_i a_{i+1})}{2}, \text{ 其中 } \text{sgn}(a) \text{ 为 } a \text{ 的符号}$$

- 序列 \mathbf{a} 的符号序列 $\text{sgn}(\mathbf{a}) := [\text{sgn}(a_1), \dots, \text{sgn}(a_t)]$, 显然 $\text{var}(\mathbf{a}) = \text{var}(\text{sgn}(\mathbf{a}))$

Example

序列 $[1, -1, 0, 3, 2, -2, 0, 1, -1]$ 的符号序列

$$\mathbf{s} = \text{sgn}(\mathbf{a}) = [1, -1, 0, 1, 1, -1, 0, 1, -1],$$

从而变号数 $\text{var}(\mathbf{a}) = \text{var}(\mathbf{s}) = 5$.

变号数

多项式组的变号数

设 $\mathcal{F} = [F_1, \dots, F_t]$ 为 $\mathbb{R}[x]$ 中的多项式序列, 则 \mathcal{F} 在 $x = a$ 处的变号数为 $\text{var}(\mathcal{F}, a) := \text{var}([F_1(a), \dots, F_t(a)])$

- 推广定义至 ∞ 和 $-\infty$.

多项式组在区间的变号数

记 $\overline{\mathbb{R}} := \mathbb{R} \cup \{-\infty, +\infty\}$, 并设 $I = (c, d)$, 其中 $c, d \in \overline{\mathbb{R}}$, 则 \mathcal{F} 在 I 上的变号数为

$$\text{var}(\mathcal{F}, I) := \text{var}(\mathcal{F}, c) - \text{var}(\mathcal{F}, d).$$

变号数

Example

考虑 $\mathbb{R}[x]$ 中的多项式序列 $\mathcal{F} = [F_1, \dots, F_5]$, 其中

$$\begin{aligned} F_1 &= x^4 - 5x^2 + 4, & F_2 &= 4x^3 - 10x, \\ F_3 &= \frac{5}{2}x^2 - 4, & F_4 &= \frac{18}{5}x, & F_5 &= 4, \end{aligned}$$

则 \mathcal{F} 在 $x = \pm\infty, \pm 1, \pm 2$ 处的符号序列及区间 $(-\infty, +\infty)$ 上的变号数为

$$\text{sgn}(\mathcal{F}, -\infty) = [1, -1, 1, -1, 1], \quad \text{sgn}(\mathcal{F}, +\infty) = [1, 1, 1, 1, 1],$$

$$\text{sgn}(\mathcal{F}, -2) = [0, -1, 1, -1, 1], \quad \text{sgn}(\mathcal{F}, 2) = [0, 1, 1, 1, 1],$$

$$\text{sgn}(\mathcal{F}, -1) = [0, 1, -1, -1, 1], \quad \text{sgn}(\mathcal{F}, 1) = [0, -1, -1, 1, 1],$$

$$\text{var}(\mathcal{F}, (-\infty, +\infty)) = \text{var}(\mathcal{F}, -\infty) - \text{var}(\mathcal{F}, +\infty) = 4.$$

Sturm 序列与变号数

Sylvester 与 Sturm 序列

设 $F \in \mathbb{R}[x]$, $P_1 = F$, $P_2 = F'$, $P_{i+1} = -\text{rem}(P_{i-1}, P_i)$. 令 t 为最后一个使得 $P_t \neq 0$ 的下标, 称 \mathcal{P} 为 F 的 Sturm 序列.

- 最后一项 P_t 即为 F 和 $F'G$ 的最大公因子.

Sturm 定理

设 $F \in \mathbb{R}[x]$, \mathcal{P} 为 F 的 Sturm 序列, $I = (c, d) \subseteq \overline{\mathbb{R}}$. 若 $F(c)F(d) \neq 0$, 则 $\text{var}(\mathcal{P}, I)$ 等于 F 在区间 I 中的实根个数.

- 任意多项式在任意区间上的实根个数可以判定!

Sturm 定理

Example

$F = x^4 - 3x^2 + 2$, 其 Sturm 序列为 $[P_1, \dots, P_5]$, 其中

$$P_1 = F = x^4 - 3x^2 + 2, \quad P_2 = F' = 4x^3 - 6x,$$

$$P_3 = -\text{rem}(P_1, P_2, x) = \frac{3}{2}x^2 - 2, \quad P_4 = -\text{rem}(P_2, P_3, x) = \frac{2}{3}x,$$

$$P_5 = -\text{rem}(P_3, P_4, x) = 2.$$

现在计算 F 在 $(0, 2)$ 上的实根数: (1) P_5 为非零常数 $\Rightarrow F$ 无重根; (2) 又由 $F(0)F(2) \neq 0$ 和 Sturm 定理 $\Rightarrow F$ 在 $(0, 2)$ 上的实根数为 $V(0) - V(2) = 2 - 0 = 2$.

实根隔离算法

算法 Isolate: $L := \text{Isolate}(F)$. 任给无平方因子的整系数多项式 $F = F(x) \in \mathbf{Z}[x]$, 本算法计算 F 的实根隔离区间 L .

I1. 计算 F 根的界 B .

I2. 计算 F 的 Sturm 序列 Θ .

I3. 命 $L := \emptyset$, $W := \{(-B, B)\}$.

I4. 若 W 为空集, 则输出 L , 且算法终止. 否则执行下列步骤:

I4.1. 任取 $(a, b) \in W$, 且命 $W := W \setminus \{(a, b)\}$. 由 Θ 计算在 $x = a$ 和 b 时 $F(x)$ 的 Sturm 序列变号数 $V(a)$ 和 $V(b)$, 并记

$$v := V(a) - V(b).$$

I4.2. 若 $v = 0$, 则返回 I4; 若 $v = 1$, 则命 $L := L \cup \{(a, b)\}$, 且返回 I4.
否则:

I4.2.1. 命 $W := W \cup \left\{ \left(a, \frac{a+b}{2} \right), \left(\frac{a+b}{2}, b \right) \right\}$.

I4.2.2. 若 $F\left(\frac{a+b}{2}\right) = 0$, 则命

$$L := L \cup \left\{ \left[\frac{a+b}{2}, \frac{a+b}{2} \right] \right\}, \quad F := \frac{F}{x - (a+b)/2}.$$

返回 I4.

实根隔离算法

课后编程练习

- ① 给定一元多项式 $F \in \mathbb{Q}[x]$ 和一个有理数 $a \in \mathbb{Q}$, 编写程序计算 F 的 **Sturm 序列 s** , 然后计算 s 在 a 处的变号数 $\text{var}(s, a)$.
- ② 给定一元多项式 $F \in \mathbb{Q}[x]$ 和任意有理数 $\epsilon \in \mathbb{Q}$, 编写程序计算 F 所有**实根的隔离区间**, 使得区间长度小于 ϵ .
- ③ 计算 $x^4 - 3x^2 + 1$ 的实根隔离区间, 使得区间长度小于 10^{-5} .

几点提示

- ① 建议用 **Maple** 软件写, 因为已经有常见的有关实根隔离的函数 (例如 `realroot`)
- ② 利用 **Maple** 软件完成作业时的提示
 - 计算 Sturm 序列时带余除法的余式可用 `rem(F, G)` 计算 (算法结果可与 **Maple** 内置函数 `sturmseq` 比较)
 - 多项式 $F(x)$ 的 Sturm 序列在区间 $[a, b]$ 上的变号数计算结果可与 **Maple** 内置函数 `sturm(F, x, a, b)` 比较
 - 计算变号数时需要用多项式 F 在某点 a 处的取值: `eval(F, x=a)`
 - 计算序列变号数时要排除其中的零元素
 - 要求隔离区间长度 $< \epsilon$, 这意味着即使算法中找到一个区间仅含一个解, 若区间不够小则仍需继续二分.
 - 计算实根的界时需要用到展开形式多项式的系数:`expand(F)` 会将多项式展开, `coeffs(expand(F))` 返回展开形式多项式的系数
- ③ 源程序需包含适量的注释