

格罗布纳基及其应用

张陈成

上海交通大学 数学科学学院

二零二二年十二月廿八日

内容提要

- ① 报告大要
- ② 楔: 平面几何问题的机器证明
- ③ 格罗布纳基简介
- ④ 应用: 图染色问题
- ⑤ 中外文翻译对照
- ⑥ 参考文献

目的 (壹)

从一类组合学问题中萃取出多项式对象, 是以将原问题转化作多项式理想问题. 例如

- 寻求平面几何问题的机器证明,
- 寻求图的染色数,
- 判断图的极大独立点集.

目的 (貳)

将格罗布纳基作为基本工具, 讨论上述多项式问题的求解理论.

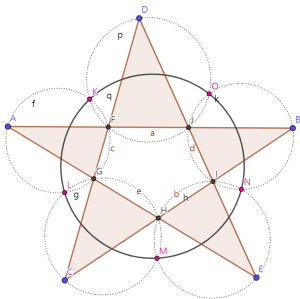
本报告不细究格罗布纳基的发展史, 请有兴致的读者移步 [\[1\]](#).

- ① 报告大要
- ② 楔: 平面几何问题的机器证明
- ③ 格罗布纳基简介
- ④ 应用: 图染色问题
- ⑤ 中英文翻译对照
- ⑥ 参考文献

平面几何问题的代数处理

例 (Z. Jiang, 2000 [4])

“假设：任意一个星形，五个三角形，外接圆交于五点. 求证这五点共圆.”



⇒ 代数问题?

平面几何问题的代数处理

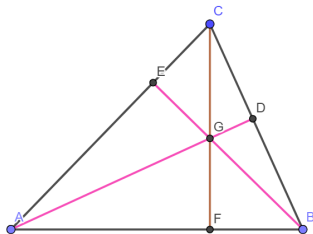
例 (任意平面三角形的三条高线是否交于一点?)

下将题设与问题转化为多项式形式求解.

- ① 不妨设 $A(0,0)$, $B(b_1,0)$, $C(c_1, c_2)$, $D(d_1, d_2)$, $E(e_1, e_2)$, $F(f_1,0)$, $G(g_1, g_2)$. 并将相应条件写作多项式形式, 如

- $XY \perp XZ$ 等价于 $(X_1 - Y_1)(X_1 - Z_1) + (X_2 - Y_2)(X_2 - Z_2) = 0$,
- $X \in YZ$ 等价于 $(X_1 - Y_1)(X_2 - Z_2) = (X_1 - Z_1)(X_2 - Y_2)$.

- ② 列出条件多项式, 如下图所示



$$\begin{aligned} E \in AC &: c_1 e_2 - c_2 e_1, \\ D \in BC &: b_1 d_2 - c_1 d_2 - c_2 b_1 + c_2 d_1, \\ AD \perp BC &: d_1(c_1 - b_1) + d_2(c_2 - b_2), \\ BE \perp AC &: c_1(e_1 - b_1) - c_2 e_2, \\ CF \perp AB &: c_1 - f_1, \\ G \in AD &: g_1 d_2 - g_2 d_1, \\ G \in EB &: g_2 e_1 + e_2 g_1 - e_2 b_1 + g_2 b_1. \end{aligned}$$

平面几何问题的代数处理

例 (接上页)

- ③ 为验证 $G \in CF$ 与否, 仅需考查是否存在 k 使得 $(g_1 - f_1)^k \in (\mathcal{F})$.
其中 \mathcal{F} 为上一步骤中的所有多项式, (\mathcal{F}) 为 \mathcal{F} 生成的理想.
- ④ 如有需要, 将上一步骤转录作平面几何的通用证明语言.

思考

试问: 如何就上述步骤三设计合理的算法? 至少, 我们熟悉以下情形

- $\mathcal{F} \in \mathbb{C}[X_1]$ 为一元多项式集, 则采用辗转相除法求解;
- $\mathcal{F} \in \mathbb{C}[X_1, \dots, X_n], \forall f \in \mathcal{F}$ 均为线性函数, 则采用高斯消元求解.

处理一般情形的难点为何? 例如 $y^3 \in (x^2, xy + y^2)$ 并不直观.

我们自然希望为多项式簇生成的理想选取合适的代表元, 例如下节介绍的格罗布纳基.

- ① 报告大要
- ② 楔: 平面几何问题的机器证明
- ③ 格罗布纳基简介
- ④ 应用: 图染色问题
- ⑤ 中外文翻译对照
- ⑥ 参考文献

例 (选取代表元集 S 的简单例子)

- 毋庸置疑, $\mathcal{F} \subseteq \mathbb{C}[X_1]$ 的代表元 (集) 为全体 $f \in \mathcal{F}$ 的最大公因子, 因为 $\mathbb{C}[X_1]$ 为主理想整环.
- 线性多项式组 \mathcal{F} 的代表元可选行阶梯形式, 如

$$\begin{cases} 3x + 3y + 9z + w, \\ x + y + 3z, \\ x + 2y + 5z + w, \end{cases} \implies \begin{cases} x + z, \\ y + 2z, \\ w. \end{cases}$$

- 直觉上, $\{X_1^2, X_2^2 - X_1, X_2\} \subseteq \mathbb{C}[X_1, X_2]$ 的代表元集可选 $\{X_1, X_2\}$.

约定 (次数向量)

若无歧义, 规定 $\mathbb{C}[X] = \mathbb{C}[X_1, \dots, X_n]$. 记各项非负的向量 $a = (a_i)_{1 \leq i \leq n}$ 为次数向量, 在 X 上的作用为 $X^a := \prod_{1 \leq i \leq n} X_i^{a_i}$. 例如 $X^{(1,0,2)} = X_1 \cdot X_3^2$.

单项式序

定义

简而言之, 多项式序无非 $\prod_{i=1}^n (\mathbb{Z}_{\geq 0})$ 上的全序关系 $<$, 满足

- ① 对任意 $a \neq 0$, 总有 $0 < a$;
- ② 若 $a < b$, 则对任意 c 总有 $a + c < b + c$.

以下是几类常用的单项式序.

定义 (字典序, 正序, 逆序)

不妨采用次数向量表示单项式. 定义

- 字典序: $a > b$ 若且惟若 $a - b$ 首非零项为正.
- 正序: $a > b$ 若且惟若 $|a| > |b|$, 或 $|a| = |b|$ 且 $a - b$ 首非零项为正.
- 逆序: $a > b$ 若且惟若 $|a| > |b|$, 或 $|a| = |b|$ 且 $a - b$ 末非零项为正.

单项式序

例

方便起见, 选取 $n = 2$. 以上三种典型的单项式序分别为

- 字典序: $1 < X_2 < X_2^2 < \cdots < X_1 < X_1 X_2 < X_1 X_2^2 < \cdots$,
- 正序: $1 < X_2 < X_1 < X_2^2 < X_1 X_2 < X_1^2 < X_2^3 < \cdots$,
- 逆序: $1 < X_1 < X_2 < X_1^2 < X_1 X_2 < X_2^2 < X_1^3 < \cdots$.

为仿照 $n = 1$ 时的辗转相除法, 需定义多项式的首要部分, 即

定义 (首项)

给定单项式序. 定义多项式 f 的主项 $\text{in}(f)$ 为次数最高的单项式.

例

例如对字典序, $\text{in}(2X_1^2 X_2 - 3X_1 X_2^3) = -2X_1^2 X_2$.

格罗布纳基

正式定义格罗布纳基前, 先介绍首项理想.

定义 (首项理想)

给定理想 I 与单项式序, 定义首项理想为 $\text{in}(I) := (\{\text{in}(f) \mid f \in I\})$.

定义 (格罗布纳基)

给定理想 $I \subseteq \mathbb{C}[X]$ 与单项式序, 称 $G = \{g_i\}_{1 \leq i \leq n}$ 为 I 关于相应单项式序的格罗布纳基, 若

$$\text{in}(I) = (\{\text{in}(g_i) \mid g_i \in G\}).$$

判断 $h \in I$ 与否即判断 (h, I) 经辗转相除后余项是否为 0. 此处

- 单项式序结构给出辗转相除的基本方向,
- $\text{in}(G) = \text{in}(I)$ 表明 G 中全体多项式的主项足够刻画理想 I 中一切多项式之主项.

插曲：如何判断 $h \in I$ 与否？

给定 $I \subseteq \mathbb{C}$ 与格罗布纳基 G , 如何判断 $h \in I$? 以下将采用基于格罗布纳的辗转相除法求解.

例 (判断 $h \in I$ 的简易算法)

- 输入 G, h % 其中 G 是有限集.
- 输出 $\{0, 1\}$ % 0 表示 $h \notin I$, 1 表示 $h \in I$.
- 当 存在 $g_i \in G$ 使得 $\text{in}(g_i) \mid \text{in}(h)$
 - 令 $h = h - \frac{\text{in}(h)}{\text{in}(g_i)} \cdot g_i$
 - 若 $h = 0$ 则 输出 1
- 输出 0

思考

上述算法的第三行为何在一定有限步后停止？

布什伯格算法

根据格罗布纳基的定义, 我们提出以下或许不显然的问题.

- ① 任意理想 $I \subseteq \mathbb{C}[X]$ 的格罗布纳基是否存在?
- ② 若存在, 如何计算之?
- ③ 若存在, 是否在某种程度上惟一?

问题一是希尔伯特基定理的直接推论. 问题二的答案即本节所介绍的布什伯格算法. 问题三移步 [3].

引入布什伯格算法前, 需完善对余数的定义.

定义 (G -同余关系)

给定格罗布纳基 G 与多项式 h , 定义同余关系

$$R_G(h) = R_G(h + fg_i), \quad \forall g_i \in G, \forall f \in \mathbb{C}[X].$$

布什伯格算法

余数自然是同余关系划分出的等价类, 下采用等价类中极小代表元定义之.

定义 (余数)

取多项式 $h \in \mathbb{C}[X]$, G 为给定的格罗布纳基.

- 若 $R_G(h) = R_G(0) := 0$, 则记整除关系为 $h \mid G$.
- 若不然, 存在与 h 同余的 h' 使得 $\text{in}(g_i) \nmid \text{in}(h')$, $\forall g_i \in G$.
此时 h' 惟一, 记作余数.

以下定义布什伯格算法中的 S -差. 特别地, 格罗布纳基在 $R_G \circ S$ 下恒为 0.

定义 (S -差)

S -差为 $\mathbb{C}[X] \times \mathbb{C}[X]$ 到 $\mathbb{C}[X]$ 的函数, 定义作

$$S(f, g) = \text{lcm}(f, g) \left(\frac{f}{\text{in}(f)} - \frac{g}{\text{in}(g)} \right).$$

布什伯格算法

例 (布什伯格算法全貌)

- **输入** $\{f_i\}_{1 \leq i \leq r} \subseteq \mathbb{C}[X]$ % 有限多项式集可指代一般理想
- **输出** G % $\{f_i\}_{1 \leq i \leq r}$ 扩充的格罗布纳基
- $G := \{f_i\}_{1 \leq i \leq r}$
- $P := \{(f_i, f_j) : 1 \leq i < j \leq r\}$ % G 中 $\binom{r}{2}$ 组无序对, 待消去
- **当** $P \neq \emptyset$ % 即 G 未被扩充至格罗布纳基
 - 任取 $(f_i, f_j) \in P$
 - $P := P - (f_i, f_j)$
 - $h := R_G(S(f_i, f_j))$ % 计算 $\{f_i, f_j\}$ 的 S -闭包
 - **若** $h \neq 0$ **则** % 将 h 纳入 G , 扩充无序对
 - $P := P \cup \{(h, g) \mid g \in G\}$
 - $G := G \cup \{h\}$
- **输出** G

例 (布什伯格算法举例)

取 $I = (x^2, xy + y^2) \subseteq \mathbb{C}[x, y]$, 采用字典序 ($x > y$).

- ① 初始化 $G := \{x^2, xy + y^2\}$, $P := \{(x^2, xy + y^2)\}$.
- ② 此时 $P \neq \emptyset$, 计算得 $R_G(S(x^2, xy + y^2)) = y^3$,
- ③ 经首次循环得 $G := \{x^2, xy + y^2, y^3\}$, $P := \{(y^3, x^2), (y^3, xy + y^2)\}$.
- ④ 经第二次循环, 得 $G := \{x^2, xy + y^2, y^3\}$, $P := \{(y^3, x^2)\}$.
- ⑤ 经第三次循环, 得 $G := \{x^2, xy + y^2, y^3\}$, $P := \emptyset$.

因此 $I = (x^2, xy + y^2)$ 的格罗布纳基为 $G := \{x^2, xy + y^2, y^3\}$.

- ① 报告大要
- ② 楔: 平面几何问题的机器证明
- ③ 格罗布纳基简介
- ④ 应用: 图染色问题
- ⑤ 中外文翻译对照
- ⑥ 参考文献

染色数问题

约定 (图)

以下约定一切图为简单图, 即有限, 无自环, 无重边, 无定向或权重的图. 记 $G(V, E)$ 为图的一般形式, V 为顶点集, E 为边集.

定义 (染色数)

图 $G(V, E)$ 可 k -染色, 若存在映射 $\varphi: V \rightarrow \mathbb{Z}_k$, 使得对任意 $v_1 \sim v_2$ 总有 $\varphi(v_1) \neq \varphi(v_2)$. 记上述最小的 k 为图的染色数 χ .

定义 (图多项式)

给定图 $G(V, E)$, 定义图多项式为

$$f_G := \sum_{\{u, v\} \in E} (u - v).$$

染色数问题

例 (K_3 的图多项式)

以 K_3 为例, 相应的图多项式为

$$f_{K_3} = (u - v)(w - u)(v - w) = - \sum_{\text{cyc}} (v - w)(u^2 - 1).$$

不难验证 $\chi(K_3) = 3$. 若 K_3 可 2-染色, 对任意 $\varphi: V(K_3) \rightarrow \mathbb{Z}_2$, 总有

$$\varphi \circ f_{K_3} = - \sum_{\text{cyc}} (\varphi(v) - \varphi(w))(\varphi(u)^2 - 1) = 0.$$

故存在 $u \sim v$ 使得 $\varphi(u) = \varphi(v)$, 矛盾. 不难总结得到以下定理

定理 (图的 k -染色判别法)

G 的染色数为 $k = \chi(G)$, 若且惟若对一切 $d < k$,

$$f_G \in (\{u^d - 1 \mid u \in V(G)\}).$$

覆盖问题

定义 (独立点集, 覆盖点集)

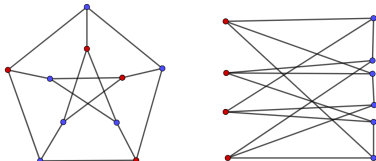
独立点集, 覆盖点集系对偶概念, 请端详定义

- 称 $U \subseteq V$ 为独立点集, 若不存在 $u, v \in U$ 使得 $\{u, v\} \in E$.
- 称 $W \subseteq V$ 为覆盖点集, 若任取 $\{s, t\} \in E$, 总有 $s \in W$ 或 $t \in W$.

有自然对应 $\{U\} \xrightarrow{1:1} \{W\}, U \mapsto U^c$.

例 (独立点集, 覆盖点集)

以下为彼得森图的极大独立点集 (红) 与极小覆盖点集 (蓝)



覆盖问题

如何用多项式描述覆盖点集 (或等价地, 独立点集)?

定义 (覆盖理想)

G 的覆盖理想为一切覆盖点集生成的理想, 定义作

$$J(G) := \bigcap_{\{u,v\} \in E} (u, v).$$

例 (C_4 的覆盖点集)

考虑 C_4 . 其中 $V(C_4) = \{a, b, c, d\}$, $E(C_4) = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, a\}\}$.

计算得相应的覆盖理想

$$\bigcap_{u \sim v} (u, v) = (a, b) \cap (b, c) \cap (c, d) \cap (d, a) = (ac, bd).$$

该理想包含一切覆盖点集, 如 abd , ac 等.

覆盖问题

定理 (染色数的等价定义)

给定图 G , 记 $\omega := \prod_{u \in V} u$ 为 G 的全覆盖, 则存在最小的正整数 d 使得

$$\omega^{d-1} \in J(G)^d.$$

此处 $d = \chi(G)$.

证明 此处根据 $\chi(G)$ 的定义考虑划分 $V = \bigcup_{i=1}^{\chi(G)} U_i$, 其中每一 U_i 均是独立点集. 等价地, U_i 为覆盖. 由是得到

$$\prod_{u \in U_i^c} u = \frac{\omega}{\prod_{u \in U_i} u} \in J(G).$$

相乘之, 得 $\omega^{\chi(G)-1} \in J(G)^{\chi(G)}$.

相反地, 可根据 $\omega^{d-1} \in J(G)^d$ 构造 d 组覆盖点集 $\{W_i\}_{i=1}^d$, 使得其无交并恰为 $d-1$ 组 V 的无交并. 因此 $\sqcup_{1 \leq i \leq d} W_i = V$. 明所欲证.





- ① 报告大要
- ② 楔: 平面几何问题的机器证明
- ③ 格罗布纳基简介
- ④ 应用: 图染色问题
- ⑤ 中英文翻译对照
- ⑥ 参考文献

中英文翻译对照

中文名称	外文名称
格罗布纳基	Gröbner basis
辗转相除法	Euclidean algorithm
高斯消元	Gaußian elimination
字典序	purely lexicographic order
正序	graded lexicographic order
逆序	graded reverse lexicographic order
首项	initial
布什伯格算法	Buchberger's algorithm
染色数	(vertex) chromatic number
独立点集	independent set
覆盖点集	(vertex) covering set
彼得森图	Petersen graph
覆盖理想	covering ideal

- ① 报告大要
- ② 楔: 平面几何问题的机器证明
- ③ 格罗布纳基简介
- ④ 应用: 图染色问题
- ⑤ 中英文翻译对照
- ⑥ 参考文献

参考文献

-  Buchberger, Bruno, *A Historic Introduction to Gröbner Bases*, 2005.
-  T. Becker, V. Weispfenning, *Gröbner Bases A Computational Approach to Commutative Algebra*, Springer, New York, 1993.
-  D. Cox, J. Little, D. O' Shea, *Ideals, Varieties and Algorithms*, Springer-Verlag, 1992.
-  R. L. Kuhn, *The Man Who Changed China: The Life and Legacy of Jiang Zemin*, Crown, 2005.

谢 谢!

Thank you!