Polynomial

(ppwwyyxxc@gmail.com)

July 8, 2013

目录

1 basic definitions

1.1 order

为单项式建立一种序关系(monomial ordering),满足:
1)全序.
2)$x^a > x^b \to x^{a+c} > x^{b+c}$
3)非空集有最小元(良序)
满足此定义的一元单项式序必为 $1 < x < x^2 < \cdots < \cdots$
对于多元单项式,有字典序(lex),全次字典序(grlex,总次数优先),全次反字典序(grvelex)
定义了序之后就可定义多元多项式除法
$f = a_1 f_1 + \cdots + a_s f_s + r, r < f_1, \cdots, f_s$.若 $f = \langle f_1, \cdots, f_s \rangle$, 则记 $r = \bar{f}^f$
这种除法的结果:
1.与 f_i 的排列顺序有关.
2.$f \in f \nrightarrow \bar{f}^f = 0$
例如:$xy^2 = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
但事实上 $xy^2 = x(y^2 - 1) \in \langle y^2 - 1, xy + 1 \rangle$

1.2 ideals

$\langle f_1, \cdots, f_s \rangle$ 的生成理想(ideals): $i = \{p_1 f_1 + \cdots + p_s f_s, p_i \in k[x_1, \cdots, x_n]\}$
如何判断两组多项式的理想相等?朴素:每个多项式都在对方的理想中.

根理想:$\sqrt{i}=\{g\in k[x_1,\cdots,x_n],\exists m,g^m\in i\}$

极大理想:$\nexists J,s.t.I\subset J\subset k[x_1,\ldots,x_n]$
商理想:$I:J=f:\forall g\in J,fg\in I$
性质: $I\cap\langle h\rangle=\langle g_1,\cdots,g_t\rangle\Rightarrow I:\langle h\rangle=\langle\frac{g_1}{h},\cdots,\frac{g_t}{h}\rangle$, 其中 $\langle g_1,\cdots,g_t\rangle$ 为 I 的 Grobner 基

求理想的交:$I\cap J=(tI+(1-t)J)\cap k[x_1,\cdots x_n]$.
证:对 $f\in RHS$, 有 $f=a_1tf_1+\cdots+a_stf_s+\cdots+a_{s+m}(1-t)g_m$
取 $t=0,1$ 即得 $f\in I,f\in J$.
反之,若 $f\in I,f\in J$, 由于 $tI+(1-t)J$ 为线性组合,立得 $f\in RHS$

1.3 Grobner's Basis

dickson's lemma:
一些单项式的理想 $I=\langle x^a:a\in A\rangle$ 总可写为有限个基的理想 $I=\langle x^{a_1},\cdots,x^{a_s}\rangle$
Def :$\mathrm{LT}(I)=\{q:\exists f\in I,\mathrm{LT}(f)=q\}$
则可证存在 $g_1,\cdots,g_s\in I,s.t.\langle\mathrm{LT}(I)\rangle=\langle\mathrm{LT}(g_1),\cdots,\mathrm{LT}(g_t)\rangle$
进一步有 Hilbert's Basis Theorem:
任一个理想可由有限个多项式生成.(多项式环是诺特环(Noetherian Domain))(基至少要有多少个?)
以及 Grobner Basis 的存在性:$G=\{g_1,\cdots,g_t\}\subset I,s.t.\forall f\in I,\exists i,\mathrm{LT}(f)|\,\mathrm{LT}(g_i)$
性质:$\forall f,\bar{f}^F$ 唯一,且 $f\in F\Rightarrow\bar{f}^F=0$
Reduced Grobner basis:$\forall p,q\in G,p\neq q,p$ 中每个单项式都不被 $\mathrm{LT}(q)$ 整除.
再加上首项系数为 1 后,称作 Monic Grobner basis,它是唯一的.

由 Hilbert,可证理想的不严格递增序列会停止.设 $I_1\subset\cdots\subset I_n\subset\cdots$
$I=\cup_{i=1}^{\infty}I_i$ 也是一个理想(证 $f,g\in I\Rightarrow f+g,pf\in I$)
I 可被有限生成.$\langle f_1,\cdots,f_s\rangle\subset I_n\subset\cdots\subset I$,则之后全取等号.

Grobner Basis 判定:(Buchberger's S-pair criterion)

$$S(f,g)=\frac{R}{\mathrm{LT}(f)}f+\frac{R}{(\mathrm{LT}(g))}g,R=Lcm(\mathrm{LT}(f),\mathrm{LT}(g))$$

则 $\langle g_1,\cdots,g_t\rangle$ 是 Grobner 基 $\Leftrightarrow\forall i,j,\overline{S(g_i,g_j)}^G=0$

Buchberger's Algorithm:
对 $G=g_1,\cdots g_s$:

REPEAT:
$\quad G'=Gx^2$
$\quad$ for each pair $\{p,q\},p\neq q$ in G',
$\quad\quad S=\overline{S(p,q)}^{G'}$
$\quad\quad$ if $S\neq0$ then $G=G\cup\{S\}$
UNTIL $G==G'$

1.4 varieties

方程组 $f_{1,\cdots,s}(x_1,\cdots,x_n)=0$ 的所有解称为 $f_1,\cdots,f_s$ 的仿射簇(affine variety)$V(f_1,\cdots,f_s)$

U,V 为仿射簇,则并与交也为仿射簇(可构造出对应的方程组)

显然 $f_1,\cdots,f_s$ 的理想 I 中任一多项式 Vanishes in $V(f_1,\cdots,f_s)$

定义 $I(V)=\{f:f(A)=0,\forall A\in V\}$

则显然 $I(V)$ 是一个理想,且 $\langle f_1,\cdots f_s\rangle\subset I(V(f_1,\cdots,f_s))$

但两者不一定相等,如 $\langle x^2,y^2\rangle\subset I(V(x^2,y^2))=I(\{0,0\})=\langle x,y\rangle$

(Strong Nullstellensatz)设 k 为代数闭域(Algebraically closed field), 则 $I(V(I))=\sqrt{I}$

但显然有 $V(I(V))=V$

线性方程组的解空间—线性簇(linear variety)(线,平面)

对一组多项式方程组的求解可应用于 Lagrange Multipliers

描述一个不可列的仿射簇,可以用参数方程.但如何由参数方程求仿射簇?

2 solve

2.1 elimination

Def: the lth elimination ideal $I_l=I\cap k[x_{l+1},\cdots,x_n]$

(Elimination Theorem):$G_l=G\cap k[x_{l+1},\cdots,x_n]$ 是 I_l 的 Grobner 基

Def: 将 $f\in I_{l-1}$ 写成 $f=c_q(x_{l+1},\cdots,x_n)x_l^q+\cdots+c_0(x_{l+1,\cdots,x_n})$. 其中 x_l^q 为 f 中 x_l 的最高次数.称 c_q 为 f 的 leading coefficient polynomial

(Extension Theorem):k 是代数闭域,$(a_{l+1}\cdots a_n)\in V(I_l)$ 若 I_{l-1} 的字典序 Grobner 基中存在的一个元素的 leading coefficient polynomials 在 $(a_{l+1},\cdots,a_n)$ 处不为 0,则此解可扩展,即 $\exists a_l, s.t.(a_l,\cdots,a_n)\in V(I_{l-1})$

对零维理想,可求其字典序 Grobner 基后找到一元多项式进行消元. 但此法若求数值解会导致之后系数误差,系数的微小误差对多项式根的数值求解影响很大, 根的个数,是否为实数都无法判断.

2.2 finite-dimensional algebra

对余数的算术操作,有:

$\bar{f}^G+\bar{g}^G=\overline{f+g}^G,\overline{fg}^G=\overline{\bar{f}^G\bar{g}^G}^G$ (乘积次数可能变大,要再取余)

由商环 $k[x_1,\ldots,x_n]/I$ 中定义陪集(coset):$[f]=f+I=\{f+h:h\in I\}$.

于是有 $\bar{f}^G=\bar{g}^G\Leftrightarrow f-g\in I\Leftrightarrow[f]=[g]$

对陪集定义对应的算术操作,则此商环有线性空间结构,称为一个代数 A.

定义这个代数的标准基:$B=\{x^\alpha:x^\alpha\notin\langle\mathrm{LT}(I)\rangle\}$

如 $G=\{x^2+\frac{3xy}{2}+\frac{y^2}{2}-\frac{3x}{2}-\frac{3y}{2},xy^2-x,y^3-y\}$ 是一组 grevlex 的 Grobner 基. $\langle\mathrm{LT}(I)\rangle=\langle x^2,xy^2,y^3\rangle$

$\Rightarrow B=\{1,x,y,xy,y^2\}$ 为 Remainder 中可能的单项

在 A 中根据乘法操作定义映射 $m_f:m_f([g])=[f][g]=[fg]$.

可证 m_f 为线性映射,$m_f = m_g \Leftrightarrow f - g \in I$

考虑 m_f 的矩阵表示,有 $m_f[i,j] = \overline{fB[j]}^G$ 中 $B[i]$ 项的系数

(Finiteness Theorem)$A = k[x_1, \dots, x_n]/I$ 为有限维 $\Leftrightarrow V(I)$ 为有限集 $\Leftrightarrow \forall i, \exists m_i \geq 0, g \in G : x_i^{m_i} = \mathrm{LT}(g)$. 并称这样的理想为零维理想

零维理想 $I, \forall i, I \cap k[x_i] \neq \emptyset$

证:重定义字典序使 x_i 最小.在 *Grobner* 基中,$\exists g, \mathrm{LT}(g) = x_i^{m_i}$, 则 g 只含 x_i

或:因为 A 有限维,$\Rightarrow S = \{1, [x_i], [x_i]^2, \cdots\}$ 线性相关.

设 $m_i = \min\{t : \{1, [x_i] \cdots, [x_i]^t\}$线性相关$\}$

$\Rightarrow \exists c, \sum_{j=0}^{m_i} c_j [x_i]^j = [0]$ 即 $\exists p_i(x_i) \in I$

由(Fitness Theorem),有求 B 的方法:

设 $S = \{x_1^{a_1} \dots x_n^{a_n} : 1 \leq a_i \leq m_i - 1\}, B = \{m \in S : \overline{m}^G = m\}$

(Theorem)设 A 为由零维理想 I 定义的商环上的代数,h_f 为 m_f 的最小多项式,则:

λ 是 $h_f(x) = 0$ 的根 $\Leftrightarrow \lambda$ 是 m_f 的特征值 $\Leftrightarrow \lambda \in \{f(x) : x \in V(I)\}$

由此,分别计算 $m_{x_1}, \cdots, m_{x_n}$ 即可解方程.

2.3 radical

求零维理想的根理想:

Reduce: $p_{red} = \dfrac{p}{(p, p')}$ 与 p 有相同的根但无重根(sqr free)

显然有 $\sqrt{\langle p \rangle} = \langle p_{red} \rangle$, 如果 p 为非零一元多项式.

$I \subset k[x_1 \dots x_n], p = \prod_{j=1}^{d} (x_1 - a_d), a_j$ 两两不同.$p_j = \dfrac{p}{x_1 - a_j}$,

则 $I + \langle p \rangle = \bigcap_j (I + \langle x_1 - a_j \rangle)$

证.i)$LHS \subset RHS$.因为属于右边交的每一个

ii) $p_j(I + \langle x_1 - a_j \rangle) \subset I + \langle p \rangle$

iii)设 $h \in RHS$,因为 p_j 全体互素,有 $h = \sum_j h_j p_j h$, 由上 ii), 知和式中的每一项 $\subset I + \langle p \rangle = LHS$.于是 $RHS = LHS$

I 为零维理想,$p_i \in I \cap \mathbb{C}[x_i]$,则 $\sqrt{I} = I + \langle p_{1,red}, \dots, p_{n,red} \rangle$

证:设 $RHS = J = J + \langle p_{1,red} \rangle = \bigcap_j (J + \langle x_1 - a_{1j} \rangle)$

$\Rightarrow J = \bigcap_{j_1, \cdots, j_n} (J + \langle x_1 - a_{1j_1}, \dots, x_n - a_{nj_n} \rangle)$

($\langle x_1 - a_{1j_1}, \dots, x_n - a_{nj_n} \rangle$) 为极大理想, 所以 $(J + \langle x_1 - a_{1j_1}, \dots, x_n - a_{nj_n} \rangle)$ 等于 $\mathbb{C}[x_1 \dots, x_n]$ 或 $\langle x_1 - a_{1j_1}, \dots, x_n - a_{nj_n} \rangle \Rightarrow J$ 为极大理想的交,仍为极大理想 $\Rightarrow J$ 为根理想

由于 p_i 的无平方部分 vanish at$V(I)$, 有 $J \subset I(V(I)) = \sqrt{I}$,又由定义, $I \subset J \Rightarrow J \subset \sqrt{I} \subset \sqrt{J}$

于是由 $J = \sqrt{J}$ 可知 $J = \sqrt{I}$.得证.