Polynomial

(ppwwyyxxc@gmail.com)

March 5, 2012

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

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 $S\neq 0$ 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?

1.5 elimination

Definition: 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