文章编号:1001-2486(2005)01-0111-04

零维理想的正则列*

戴清平

(国防科技大学 理学院,湖南 长沙 410073)

摘 要 求一个多元多项式环的理想的正则列是非常重要和困难的问题。在字典序下,一个零维理想的 Grøbner 基中含有一个极大正则列,并且这个正则列是与顺序没有关系的。零维理想正则列的求出建立在 Grøbner 基的可计算性和首项理想的根理想的准素分解算法上。

关键词 单项式理想;Grøbner 基;零维理想;正则列

中图分类号 O187 **文献标识码** A

The Regular Sequence of Zero Dimension Ideals

DAI Qing-ping

(College of Science, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: It is very important and diffcult to obtain the ideal regular sequence of polynomial ring. In the lexical order a zero dimension ideal Grøbner has a maximal orderless regluar sequence. We can obtain the regular sequence owing to the calculability of Grøbner bases and the method of the primary factor of the radical initial ideal.

Key words: monomial ideals; Grøbner bases; zero dimension ideals; regular sequence

给定环 $S=k[x_1,\cdots,x_n]$(k 是代数封闭域)的真理想 I,找 I 的正则列是非常重要和困难的问题。我们从零维理想 I 的 Grøbner 基中找到了它的正则列。

定义 1 理想 I 满足下列等价条件中的一个,就称为单项式理想:

(1) I 由单项式生成;(2) 如果 $f=\sum_{\alpha\in N^n}k_\alpha x^\alpha\in I$,那么 $x^\alpha\in I(k_\alpha\neq 0)$;(3) I 是 torus-fixed 如果 $(c_1,\cdots,c_n)\in(k^*)^n$,那么 I 在变换 $x_i\to c_ix_i$ 下不变。

定义 2 假设 R 是一个诺特环,一个元素 $a\in R$ 称为 R-正则。如果 $0\neq x\in R$ 都有 $ax\neq 0$,而且 $aR\neq R$,环 R 的一个序列 $a_1,\cdots,a_n$ 称为正则列。如果下列条件满足:

(1) a_1 是 R-正则,a_i 是 $R/(a_1,\cdots,a_{i-1})(i=2,\cdots,n)$ 正则;(2) $(a_1,\cdots,a_n)R\neq R$。

令 N 是非负整数集合,n 是一个给定的正整数,$x_1,x_2,\cdots,x_n$ 表示环 S 上的 n 个变元。

$$T^n=T(x_1,x_2,\cdots,x_n)=\{x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}\mid\alpha_i\in\mathbf{N},i=1,\cdots,n\},$$

即 T^n 是 n 个变元 $x_1,x_2,\cdots,x_n$ 的幂积的集合。记 $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}=X^\alpha$,其中 $X=(x_1,x_2,\cdots,x_n)$,$\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in N^n$。

所谓 σ 是集合 T^n 上的一个全序(total order),是指对任意给定的 T^n 中的两个元素 X^α 和 X^β,下面的三个关系有且只有一个成立:

$$X^\alpha<_\sigma X^\beta,\quad X^\alpha=X^\beta,\quad X^\beta<_\sigma X^\alpha$$

如果无须特别标注 σ,上式可简记为

$$X^\alpha<X^\beta,\quad X^\alpha=X^\beta,\quad X^\beta<X^\alpha$$

集合 T^n 上的全序 σ 称为良序(well-ordering),如果 T^n 的每个非空子集合都有最小元,即对 T^n 的任何非空子集 A,必存在元素 $X^\alpha\in A$,使得对所有 $X^\beta\in A$,$X^\alpha\leqslant_\sigma X^\beta$。

* 收稿日期:2004-09-27

作者简介:戴清平(1966—),男,副教授。

定义 3 集合 T^n 上的序 σ 称为项序(term order),是指 σ 是一个全序,同时满足下面的两个性质:

(1) 对所有 $X^\beta \in T^n$ 和 $X^\beta \neq 1$,都有 $X^\beta >_\sigma 1$。

(2) 对任何 $X^\alpha, X^\beta, X^\gamma \in T^n$,如果 $X^\alpha <_\sigma X^\beta$,则 $X^\alpha X^\gamma <_\sigma X^\beta X^\gamma$。

用 Hilbert 基定理,可证明项序必是良序。

最常用三种序是字典序:(lexicographical order),简记为 lex;次数字典序(degree lexicographical order),简记为 deglex;次数反字典序(degree reverse lexicographical order),简记为 degrevlex。

设 $<\sigma$(简记为 $<$)为 S 上的一个项序,多项式环 S 中的任一个非零多项式 f,总可惟一地表示为

$$f = a_1 X^{\alpha_1} + a_2 X^{\alpha_2} + \cdots + a_r X^{\alpha_r}$$

其中,$0 \neq a_i \in k$,$X^{\alpha_i} = x_1^{\alpha_{i1}} \cdots x_n^{\alpha_{in}}$ $(1 \leqslant i \leqslant r)$。

$lp(f) = X^{\alpha_1}$,即 $lp(f)$ 表示 f 的首项幂积; $lc(f) = a_1$,即 $lc(f)$ 表示 f 的首项系数;

$lt(f) = a_1 X^{\alpha_1}$,即 $lt(f)$ 表示 f 的首项; $c(f, X^\alpha)$ 为幂积 X^α 在 f 中的系数;

$Supp(f) = \{X^\alpha \in T^n \mid c(f, X^\alpha) \neq 0\}$,为在 f 中出现的幂积的集合。

定义 4 对于给定的三个多项式 f, g, h,其中 $g \neq 0$,f 模 g 一步约化为 h,用 $f \xrightarrow{g} h$ 表示,当且仅当 $lp(g)$ 是 f 中某一非零单项式(也称为项)X 的因子,并且 $h = f - \dfrac{X}{lt(g)} g$。

定义 5 令 $f, h, f_1, \cdots, f_s$ 是 S 中的多项式,且对 $i = 1, 2, \cdots, s$,$f_i \neq 0$,令集合 $F = \{f_1, \cdots, f_s\}$。f 模 F 约化为 h,用 $f \xrightarrow{F} {}_+ h$ 表示,当且仅当下式成立:

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \longrightarrow \cdots \xrightarrow{f_{i_t}} h_t = h$$

定义 6 设多项式 $r \in S$,$F = \{f_1, \cdots, f_s\} \subseteq S \setminus \{0\}$,如果 $r = 0$ 或者 r 模 F 不能约化,即 $lt(f_i)$ $(i = 1, 2, \cdots, s)$ 中的任何一个都不是在 r 中出现的幂积的因子,则称多项式 r 相对 F 是既约的(reduced)。进而,如果 $f \xrightarrow{F} {}_+ r$ 和 r 相对 F 是既约的,则称 r 为 f 相对 F 的剩余(remaider)或余多项式.

定义 7 设 I 是环 S 中任意给定的一个非零理想,$G = \{g_1, \cdots, g_t\}$ 是 I 中非零多项式的有限集合。称 G 是理想 I 的 Grøbner 基(Grøbner basis)当且仅当对 I 中的每个非零多项式 f,存在 i $(1 \leqslant i \leqslant t)$,使得 $lp(g_i) \mid lp(f)$。

定义 8 令 I 是环 S 中的非零理想,$lt(I) = < ltf \mid f \in I >$,$lt(I)$ 称为首理想(initial ideal)。

引理 1[8] 令 I 是环 S 中的非零理想,$G = \{g_1, \cdots, g_t\} \subseteq I \setminus \{0\}$,设 $lt(G) = (ltg \mid g \in G)$,则下面的叙述是等价的:

(1) G 是 I 的 Grøbner 基;(2) $f \in I$ 当且仅当 $f \xrightarrow{G} {}_+ 0$;(3) $f \in I$ 当且仅当存在 $h_1, \cdots, h_t \in S$,使得 $f = \sum_{i=1}^{t} h_i g_i$,$lp(f) = \max\{lp(h_i) lp(g_i) \mid i = 1, 2, \cdots, t\}$;(4) $lt(G) = lt(I)$。

推论 1[8] 设 I 是环 S 中的理想,$G = \{g_1, \cdots, g_t\} \subseteq I \setminus \{0\}$。如果 G 是 I 的 Grøbner 基,则 $I = (g_1, \cdots, g_t) = (G)$,即 I 的 Grøbner 基必定是 I 的生成元集合。

推论 2[8] 设 G 是环 S 中 I 的 Grøbner 基,对任何 $f \in S$,$f \xrightarrow{G} {}_+ r$,其中 r 相对 G 是既约,则 r 由 f 和 G 惟一确定。

定义 9 设 I 是 $k[x_1, \cdots, x_n]$ 的理想,对于字典序而言,如果 $T(u_1, u_2, \cdots, u_s) \cap lt(I) = \phi$,称 $\{x_1, \cdots, x_n\}$ 的子集 $\{u_1, u_2, \cdots, u_s\}$ 为模 I 强独立的,称 $d = \max\{|U| \mid U \subset \{x_1, \cdots, x_n\}$,并且 U 是模 I 强独立的$\}$ 是理想 I 的强维数。

引理 2[11] 设 I 是 $k[x_1, \cdots, x_n]$ 的理想,则 $d = \dim(I) = \dim(lt(I))$。

引理 3 设 $I = (X^{\alpha_1}, \cdots, X^{\alpha_r})$ 是单项式理想,下列条件等价:(1) $ht(I) = r$;(2) $X^{\alpha_1}, X^{\alpha_2}, \cdots, X^{\alpha_r}$ 两两相对素;(3) $X^{\alpha_1}, X^{\alpha_2}, \cdots, X^{\alpha_r}$ 为无序正则列。

证明 (1)$\Rightarrow$(2):

设 $Y_i = x_{i1} x_{i2} \cdots x_{it_i}$ 为 X^{α_i} 中出现的不定元之积,$J = (Y_1, \cdots, Y_r)$,显然有 $J = ((x_{11}) \cap \cdots \cap (x_{1t_1}), \cdots,$

$(x_{r1})\cap\cdots\cap(x_{rt_r}))$。一般地,设 $I_1,\cdots,I_s,J_1,\cdots,J_t$ 是理想,有:

$$\left(\bigcap_{l=1}^{s}I_l,\bigcap_{m=1}^{t}J_m\right)\subseteq\bigcap_{l,m}(I_l,J_m)$$

事实上 $$\bigcap_{l,m}(I_l,J_m)=\bigcap_{l,m}(I_l+J_m)\supseteq\bigcap\bigcap_{l=1}^{s}I_l+\bigcap_{m=1}^{t}J_m=\left(\bigcap_{l=1}^{s}I_l,\bigcap_{m=1}^{t}J_m\right)$$

在我们的问题中 $$J\subseteq\bigcap_{\substack{1\leqslant i_j\leqslant t_j\\1\leqslant j\leqslant r}}(x_{1i_1},\cdots,x_{ri_r})\triangleq Q$$

考虑零点集有 $V(I)=V(\sqrt{I})=V(J)=V(Q)$,$Q=\sqrt{Q}$,因此$\sqrt{I}=Q$。

在$\sqrt{I}$的理想交表示中,相同者保留一个,有包含关系的把母集合去掉,剩下的素理想交为$\sqrt{I}$的极小准素分解。因此 $$ht(\sqrt{I})=\min_{\substack{1\leqslant i_j\leqslant t_j\\1\leqslant j\leqslant r}}|\{x_{1i_1},\cdots,x_{ri_r}\}|$$

由 $ht(\sqrt{I})=ht(I)=r$,说明每个素理想中无相同不定元,从而 X^{α_1}, X^{α_2},$\cdots$,X^{α_r}两两相对素。

(2)$\Rightarrow$(3)

说明 X^{α_r}是 $k[x_1,\cdots,x_n]/(X^{\alpha_1},\cdots,X^{\alpha_{r-1}})$的非零因子,其余类推。

设 $X^{\alpha_r}f=\sum_{i=1}^{r-1}g_iX^{\alpha_i}$,不妨设$f$已经不能合并同类项,同样可以假设右边在展开后不能再合并。设 $X^{\beta}\in Supp(f)$,存在某个 $1\leqslant i_0\leqslant r-1$ 使得 $X^{\alpha_r}X^{\beta}=X^{\alpha_{i_0}}X^{\gamma}$ 由于 X^{α_r} 与 $X^{\alpha_{i_0}}$ 相对素,故 $X^{\alpha_r}\mid X^{\gamma}$,从而有 $X^{\beta}\in(X^{\alpha_{i_0}})$,故 $f\in(X^{\alpha_1},\cdots,X^{\alpha_{r-1}})$。

显然上述证明对 X^{α_1}, X^{α_2},$\cdots$,X^{α_r}的任一排列都对。

(3)$\Rightarrow$(1):

由 $S=k[x_1,\cdots,x_n]$的 C-M 性有 $ht(I)=depth(I)=r$。

推论 3 设 $I=(X^{\alpha_1},\cdots,X^{\alpha_r})$是单项式理想,$X^{\gamma}$ 是单项式,那么

$$ht(I,X^{\gamma})\leqslant ht(I)+1$$

证明 类似于引理 3 中(1)$\Rightarrow$(2)的证明。

注 1 推论 3 的一般情况不成立.

例 1 $I=(x_1(x_n-1),\cdots,x_{n-1}(x_n-1),x_n)$,$J=(x_1(x_n-1),\cdots,x_{n-1}(x_n-1))$,则 $ht(J)=1$, $ht(I)=n$.

注 2 设(A,m,k)是 C—M 局部环,$I\subset m$,$y\in m$,那么

$$ht(I,y)\leqslant ht(I)+1$$

证明 设 $I=(x_1,\cdots,x_n)$,$r=depth(I,y)$,考虑 koszul 复形与 depth 的关系,r 为使 $H^r(K(x_1,\cdots,x_n,y))\neq0$ 的最小整数$\rightarrow H^{r-2}(K(X,y))\rightarrow H^{r-2}(K(X))\xrightarrow{\pm y}H^{r-2}(K(X))\rightarrow H^{r-1}(K(X,y))$。因为首位两项都是零,由 Nakayama 引理有 $H^{r-2}(K(X))=0$,因此 $depth(I)\geqslant r-1$,$depth(I,y)\leqslant depth(I)+1$. 由 C—M 性得结论。

定理 1 在环 $S=k[x_1,\cdots,x_n]$中,$F=\{g_1,\cdots,g_s\}$,$I=(F)$,那么:$lp(g_i)$与 $lp(g_j)$ $(i\neq j)$相对素$\Leftrightarrow$(1)F 为 I 的 Grøbner 基;(2)$ht(I)=s$。

证明 $\Rightarrow$:

设 $g_i=lt(g_i)+p_i(1\leqslant i\leqslant s)$,$S(i,j)=lt(g_i)(lt(g_j)+p_j)-lt(g_j)(lt(g_i)+p_i)=lt(g_i)p_j-lt(g_j)p_i$,如果 $lt(lt(g_i)p_j)=lt(lt(g_j)p_i)$,即 $lt(g_i)lt(p_j)=lt(g_j)lt(p_i)$,由于 $lt(g_i)$与 $lt(g_j)$相对互素,因此 $lt(g_i)\mid lt(p_i)$,矛盾。

$\Leftarrow$:

由引理 2 和引理 3 得证。

推论 4 设 $G=\{g_1,\cdots,g_l\}$为理想 I 的 Grøbner 基,$\begin{cases}s=\max\{r\mid X^{\alpha_i}\in lt(I),1\leqslant i\leqslant r,X^{\alpha_i}\text{与 }X^{\alpha_j}\text{互素}\}\\t=\max\{u\mid X^{\alpha_i}\in lt(G),1\leqslant i\leqslant u,X^{\alpha_i}\text{与 }X^{\alpha_j}\text{互素}\}\end{cases}$,那么 $t=s\leqslant ht(I)$。

证明 设 $\{f_1,\cdots,f_s\}\subset I$,且其首项两两相对互素,由定理 1 有 $ht(J)=s\leqslant ht(I)$。

由于 $lt(g_{l_i}) \mid lt(f_i)$，$1 \leqslant i \leqslant s$，$1 \leqslant l_i \leqslant l$，因为 $lt(f_i)$ 与 $lt(f_j)$ 相对互素，所以 $lt(g_{l_i})$ 与 $lt(g_{l_j})$ 相对互素，故 $s \leqslant t$，另外，显然有 $s \geqslant t$，因此 $s = t$。

t 与 $ht(I)$ 能相差多少，这是个诱人的问题。但是下面的例子给出了一个可悲的结论。

例 2 $I = (Y_1, Y_2, Y_3, Y_4)$ 是 $k[x_1, \cdots, x_6]$ 的理想，$Y_1 = x_1x_2x_3$，$Y_2 = x_1x_4x_5$，$Y_3 = x_2x_4x_6$，$Y_4 = x_3x_5x_6$，$\{Y_1, Y_2, Y_3, Y_4\}$ 为 I 的 Grøbner 基，且两两不相对互素，但是 $ht(I) = 2$。

一般地，利用上述方法可以构造环 $k[x_1, \cdots, x_{n(2n-1)}]$ 中的单项式理想 $I = (Y_1, Y_2, \cdots, Y_{2n})$，两两不相对互素，但是 $ht(I) = n$。

定理 2 设 $F = \{g_1, \cdots, g_s\}$ 为理想 I 的 Grøbner 基，$ht(I) = s$，那么 $g_1, \cdots, g_s$ 为无序正则列。

证明 说明 g_s 是 $k[x_1, \cdots, x_n]/(g_1, \cdots, g_{s-1})$ 的非零因子，其余类推。

设 $g_s f \in (g_1, \cdots, g_{s-1}) = J$，由定理 1 知道 $lt(g_i)$ 与 $lt(g_j)$ 相对互素，且 $\{g_1, \cdots, g_{s-1})\}$ 为 J 的 Grøbner 基. 对 f 施以除算法。如果余项 $r \neq 0$，$g_s r \in J$，$lt(g_s)lt(r) \in lt(J)$，那么存在 $g_{i_0}(1 \leqslant i_0 \leqslant s-1)$，$lt(g_s)lt(r) = lt(g_{i_0})X^\beta$，由于 $lt(g_s)$ 与 $lt(g_{i_0})$ 相对互素，知道 $lt(g_{i_0}) \mid lt(r)$，矛盾。

推论 5 设 $\{f_1, \cdots, f_s\} \subset k[x_1, \cdots, x_n]$，如果 $lt(f_i)$ 与 $lt(f_j)$ 相对互素，那么 $\{f_1, \cdots, f_s\}$ 是无序正则列。

定理 3 $\dim(I) = 0$，那么从 I 的 Grøbner 基中可以选出无序极大正则列。

证明 $\dim(I) = 0 \Leftrightarrow T(x) \cap lt(I) \neq \phi \Leftrightarrow T(x) \cap \{lt(g_1, \cdots, g_s)\} \neq \phi$

其中，$x \in \{x_1, \cdots, x_n\}$，$T(x)$ 为 x 生成的单项式集合，$G = \{g_1, \cdots, g_s\}$ 为 I 的 Grøbner 基，从而存在正整数 $k_1, \cdots, k_n$ 使得 $x_i^{k_i} = lt(g_{j_i})(1 \leqslant j_i \leqslant s)$。由定理 2 知 $g_{j_1}, \cdots, g_{j_n}$ 为无序极大正则列。

例 3 $I = (x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1)$，$x > y > z$。

I 的 Grøbner 基：$G = \{g_1, g_2, g_3, g_4\}$，$g_1 = x + y^2 + z - 1$，$g_2 = y^2 - y - z^2 + z$，$g_3 = 2yz^2 + z^4 - z^2$，$g_4 = z^6 - 4z^4 + 4z^3 - z^2$

$ht(I) = 3$，$\{g_1, g_2, g_4\}$ 是与序无关的极大正则列。下面证明 $\{g_1, g_2, g_3\}$ 也是极大正则列。设 $J = (g_1, g_2)$，令 $g_3 f \in J$，不妨先对 f 进行除算法. 设 $f = yh_1(z) + h_2(z)$，$g_3 f = 2g_2 z^2 h_1(z) + T$，$T \in J$，其中

$$T = y(z^4h_1(z) + z^2h_1(z) + 2z^2h_2(z)) + (2z^4h_1(z) - 2z^3h_1(z) + z^4h_2(z) - z^2h_2(z))$$

如果 $h_1(z) \neq 0$ 或 $h_2(z) \neq 0$，则 $lt(T) \notin lt(J)$，从而，与 $T \in J$ 矛盾，因此得证。

参 考 文 献：

[1] Adams W W, Loustaunau P. An Introduction to Grøbner Bases[M]. AMS, 1994.

[2] Becker T, Weispfenning V, Grøbner Bases[M]. Springer-Verlag, New York, 1993.

[3] Cox D, Little J, O'Shea D. Using Algebraic Geometry[M]. Springer-Verlag, New York, 1998.

[4] Bayer D, Stillman M. Computation of Hilbert Functions[J]. J. Symbolic Comput., 1992, 14(1): 31-50.

[5] Bruns W, Herzog J U. Cohen-Macaulay Rings[M]. Cambridge University Press, Cambridge, 1993.

[6] Eisenbud D. Commutative Algebra with a View toward Algebraic Geometry[M]. Springer-Verlag, New York, 1995.

[7] Cox D, Little J, O'Shea D. Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, Second Edition. Undergraduate Texts in Mathematics[M]. Springer-Verlag, New York, 1997.

[8] 刘木兰. Grøbner 基理论及其应用[M]. 北京: 科学出版社, 2000.

[9] 何青. 计算代数[M]. 北京: 北京师范大学出版社, 1997.

[10] Kredel H, Weispfenning V. Computing Dimension and Independent Sets for Polynomial Ideal[J]. J. Symbolic Comput., 1988, 6(2-3): 210-248.

[11] Bayer D, Stillman M. A Criterion for Detecting M-regularity[J]. Invent. Math, 1987, 87: 1-11.

[12] Kollar J. Sharp Effective Nullstellensatz[J]. J. Amer. Math. Soc., 1998, 1(4).

[13] Eisenbud D. Open Problems in Computational Algebraic Geometry[A]. Proceedings of the Cortona Conference on Computational Algebraic Geometry(Cambridge), 1993: 49-70.

[14] Eisenbud D, Sturmfels B. Finding Sparse Systems of Parameters[J], J. of Pure and Applied Algebra, 1994, 94: 143-157.