

实多项式方程有解的非标准判定^{*}

曾广兴

(南昌大学数学系, 南昌 330047)

摘要 对于一个系数在可计算序域上的多元多项式方程, 给出了该方程有实解的两个判别定理. 在此基础上研究了二元多项式, 从而给出了判定二元多项式的实零点存在性以及半定性的有效方法. 此外, 借助于计算机, 处理了几个有关实例. 处理手段是: 通过无限小量的引进, 将问题所涉及的系数域扩充为一个可计算的非 Archimedes 序域.

关键词 计算代数几何 实系数多项式 可解性 半定多项式 无限小量

判定实多项式方程是否有实解, 是实代数几何在计算方面的一个基本重要课题. 正如文献[1]所指出, 这一课题与有序几何中定理机器证明密切相关. 理论上, 熟知的 Tarski-Seidenberg 原理^[2,3] 提供了一个判定方法. 然而, 这种方法会派生出大量由方程与不等式构成的关系式组, 以致难于实施. 文献[4,5]给出了实多项式的完全判别系统, 从而通过一组由多项式系数构成的显式表达式对多项式的根进行了完全的分类, 并在此基础上对实多项式方程和不等式进行了许多有意义的工作.

本文突破给定多项式所在的原来系数域的局限, 将问题的讨论从具有实闭包 R 的原系数域 K 扩大到一个具有实闭包 $R_{\langle n \rangle}$ 的序域 $K_{\langle n \rangle}$, 这里 $K_{\langle n \rangle}$ 是一个可计算的包含无限小正元素 $t_1, t_2, \dots, t_n$ 的非 Archimedes 序域. 正因为这一缘故, 称本文中的方法是非标准的. 作为本文的主要结果, 建立了如下两个关于实多元多项式有实零点的判别定理:

定理 1 设 $f(X)$ 是 K 上 n 元多项式, $n \geq 2$, 则方程 $f(X)=0$ 在 R 中有解, 当且仅当如下 4 个叙述之一成立:

- (1) 方程 $f(0, x_2, \dots, x_n)=0$ 在 R 中有解;
- (2) 对于某个 $j \in \{2, \dots, n\}$, 方程 $f(x_1, \dots, x_{j-1}, t^{-1}, x_{j+1}, \dots, x_n)=0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (3) 对于某个 $j \in \{2, \dots, n\}$, 方程 $f(x_1, \dots, x_{j-1}, -t^{-1}, x_{j+1}, \dots, x_n)=0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (4) 方程组 $f(X)=0, \frac{\partial f(X)}{\partial x_i}=0 (i=2, \dots, n)$ 在 R 中有解.

定理 2 设 $f(X)$ 是 K 上 n 元多项式, $n \geq 2$, 则方程 $f(X)=0$ 在 R 中有解, 当且仅当如下 4 个叙述之一成立:

- (1) 方程 $f(t^{-1}, x_2, \dots, x_n)=0$ 在 $R_{\langle 1 \rangle}$ 中有解;

- (2) 对于某个 $j \in \{2, \dots, n\}$, 方程 $f(x_1, \dots, x_{j-1}, t^{-1}, x_{j+1}, \dots, x_n) = 0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (3) 对于某个 $j \in \{2, \dots, n\}$, 方程 $f(x_1, \dots, x_{j-1}, -t^{-1}, x_{j+1}, \dots, x_n) = 0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (4) 方程组 $f(X) = 0, \frac{\partial f(X)}{\partial x_i} = 0 (i = 2, \dots, n)$ 在 R 中有解.

定理 2 是定理 1 的一种变形, 且它在 $f(X)$ 是对称多项式时特别适用. 在上面定理的基础上, 给出了二元实多项式的实零点存在性以及半定性的有效判定方法. 应该指出, 通过一些技术上的处理, 这些方法原则上都可推广到 $n (> 2)$ 元多项式, 对此将另文讨论. 此外, 作为这些方法的应用, 使用计算机代数系统 Maple V Release 4^[6] 处理了有关实例.

1 实多项式方程有解的判别定理的证明

本节将证明定理 1 和 2. 为此, 需要下面的基本概念和有关事实.

依照文献[7]中定义 4.18, 一个序域 $(K, \leq)$ 称作可计算的, 如果 K 是一个可计算域, 且 $\leq$ 是 K 的一个可判定序. 此时, 可认定 $\mathbb{Q} \subseteq K$, 这里 $\mathbb{Q}$ 为有理数域. 设 $t \doteq t_1, \dots, t_n$ 是域 K 上 n 个未定元, 且令 $K_{\langle n \rangle} \doteq K(t_1, t_2, \dots, t_n)$, 则序 $\leq$ 可以唯一地拓展成域 $K_{\langle n \rangle}$ 的一个序, 仍记作 $\leq$, 使得 t_i 关于 $K_{\langle i-1 \rangle} \doteq K(t_1, \dots, t_{i-1})$ 是正的无限小, $i = 1, \dots, n$. 显然, 序域 $(K_{\langle n \rangle}, \leq)$ 也是可计算的. 事实上, 对于 $K_{\langle n \rangle}$ 中非零元素 f/g , 其中 $f, g \in K[t_1, \dots, t_n]$, $f/g < 0$ 当且仅当多项式 fg 关于字典序 $t_1 \ll t_2 \ll \dots \ll t_n$ 的最低项系数为负. 用 R 和 $R_{\langle n \rangle}$ 分别表示序域 $(K, \leq)$ 和 $(K_{\langle n \rangle}, \leq)$ 的实闭包. 当然, 认为 $R \subset R_{\langle n \rangle}$. 此外, 用 $R_{\langle i \rangle}$ 表示 $K_{\langle i \rangle}$ 在 $R_{\langle n \rangle}$ 中的代数闭包, $i = 1, \dots, n-1$. 由文献[8]中引理 3.13 知, $R_{\langle i \rangle}$ 实际上也是 $K_{\langle i \rangle}$ 关于序 $\leq$ 的实闭包. 显然, $R \subset R_{\langle 1 \rangle} \subset \dots \subset R_{\langle n \rangle}$.

作实闭域 $R_{\langle n \rangle}$ 的如下两个子集:

$$A_{\langle n \rangle} \doteq \{z \in R_{\langle n \rangle} \mid \text{对于 } R \text{ 中某个正元素 } D, -D \leq z \leq D\},$$

$$M_{\langle n \rangle} \doteq \{z \in R_{\langle n \rangle} \mid \text{对于 } R \text{ 中任意正元素 } D, -D \leq z \leq D\}.$$

由序 $\leq$ 的结构可知, $R \subset A_{\langle n \rangle}$, 且 $t_i \in M_{\langle n \rangle}$, $i = 1, \dots, n$. 根据实赋值的熟知结论 (参见文献[9]中命题 1.3 与文献[10]中 §5 内有关定理), $A_{\langle n \rangle}$ 是域 $R_{\langle n \rangle}$ 的一个实赋值环, $M_{\langle n \rangle}$ 是 $A_{\langle n \rangle}$ 的赋值理想. 此外, $(A_{\langle n \rangle}, M_{\langle n \rangle})$ 和序 $\leq$ 是相容的, 换句话说, $A_{\langle n \rangle}, M_{\langle n \rangle}$ 关于序 $\leq$ 都是 $R_{\langle n \rangle}$ 的凸子集. 注意到 $A_{\langle n \rangle}$ 的剩余域 $A_{\langle n \rangle}/M_{\langle n \rangle}$ 同构于 R , 从而存在一个从 $A_{\langle n \rangle}$ 到 R 的同态映射 π , 使得对于每个 $f \in R[t_1, \dots, t_n]$, $\pi(f(t_1, \dots, t_n)) = f(0, \dots, 0)$.

在本文中, 将使用上述术语和记号, 不再另加说明.

现设 $f(X) \in K[X] \doteq K[x_1, \dots, x_n]$ 是一个正次数 n 元多项式. 令 $V_R(f, x_i) \doteq \{a_i \in R \mid \exists a_j \in R, j = 1, \dots, i-1, i+1, \dots, n, f(a_1, a_2, \dots, a_n) = 0\}$, 这里 $i = 1, \dots, n$. 由文献[11]中定理 2.12 和例 2.14(b) 知, 当方程 $f(X) = 0$ 在 R 中有解时, $V_R(f, x_i) (i = 1, \dots, n)$ 都是 R 的非空半代数子集, 且都是由 R 中有限个不相交 (开或闭或半开半闭) 区间以及点构成的并集. 对于 $a \in R$, 记作 $]a, a[\doteq \{a\}$, 从而单点集可看作左, 右端点相同的闭区间. 如若 $V_R(f, x_i)$ 有某两个区间, 其中一个的右端点和另一个的左端点相同, 且一开一闭, 则可以将两者合并为一个大区间. 因此, 假定 $V_R(f, x_i)$ 中任何两个区间都不具有如此情形, $i = 1, \dots, n$. $V_R(f, x_i)$ 的一个区间的端点 a 称作有限端点, 若 $a \neq -\infty$ 且 $a \neq +\infty$. 显然, 当 $V_R(f, x_i) \neq R$ 时, $V_R(f, x_i)$ 必有有限

端点. 对于有限端点, 有如下断言:

引理 1 设 a_1 是 $V_R(f, x_1)$ 的一个有限闭端点, 且 $a_2, \dots, a_n \in R$, 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则方程组 $f(X) = 0, \frac{\partial f}{\partial x_i} = 0 (i = 2, \dots, n)$ 在 R 中有解 $(a_1, a_2, \dots, a_n)$.

证 由于端点 a_1 不是 $V_R(f, x_1)$ 的内点, 从而对于点 a_1 的任意开邻域 S , 均有 $S \not\subseteq V_R(f, x_1)$. 假若对于某个 $j \in \{2, \dots, n\}$, $\frac{\partial f}{\partial x_j}(a_1, a_2, \dots, a_n) \neq 0$, 不失一般性, 不妨设 $j = n$. 根据适合实闭域的隐函数定理 (参见文献 [11] 中的推论 2.9.6), 存在 $(a_1, \dots, a_{n-1})$ 在序拓扑空间 R^{n-1} 中的一个开邻域 Δ , a_n 的一个开邻域 T 以及一个从 Δ 到 T 的函数 (映射) φ , 使得 $\varphi(a_1, \dots, a_{n-1}) = a_n$ 且对于每个 $(x_1, \dots, x_{n-1}, x_n) \in \Delta \times T, f(x_1, \dots, x_{n-1}, x_n) = 0$ 当且仅当 $x_n = \varphi(x_1, \dots, x_{n-1})$. 由空间 R^{n-1} 的拓扑结构, 存在点 a_i 的一个开邻域 $S_i (i = 1, \dots, n-1)$, 使得 $S_1 \times \dots \times S_{n-1} \subseteq \Delta$. 这样, 显然有 $S_1 \subseteq V_R(f, x_1)$, 矛盾. 因此, 对于每个 $i = 2, \dots, n, \frac{\partial f}{\partial x_i}(a_1, a_2, \dots, a_n) = 0$.

引理 2 设 $V_R(f, x_1)$ 有一个有限开端点, 则对于某个 $j \in \{2, \dots, n\}$, 方程

$$f(x_1, \dots, x_{j-1}, t^{-1}, x_{j+1}, \dots, x_n) = 0$$

或

$$f(x_1, \dots, x_{j-1}, -t^{-1}, x_{j+1}, \dots, x_n) = 0$$

在 $R_{\langle 1 \rangle}$ 中有解.

证 不失一般性, 设 a_1 是 $V_R(f, x_1)$ 的一个左侧有限开端点, 则 $a_1 \notin V_R(f, x_1)$, 同时必有一个开区间 $a_1, c (\subseteq V_R(f, x_1))$, 其中 $c \in R$, 使得 $a_1 < c$. 此时, 可以断言: 对于某个 $j \in \{2, \dots, n\}$, $V_R(f, x_j)$ 不是一个有界集. 假若不然, 则 R 中存在一个正元素 D , 使得 $-D < y < D, \forall y \in V_R(f, x_i), i = 2, \dots, n$. 于是, 有如下语句在 R 中成立:

$$\forall x_1 (a_1 < x_1 < c) \Rightarrow \exists (x_2, \dots, x_n) (f(x_1, x_2, \dots, x_n) = 0 \text{ 且 } -D < x_i < D, i = 2, \dots, n).$$

注意到 $R \subset R_{\langle 1 \rangle}$, 从而由适合实闭域的转移定理 (参见文献 [11] 中的命题 5.2.3), 上面语句在 $R_{\langle 1 \rangle}$ 中也成立. 令 $\alpha_1 = a_1 + t$, 则 $\alpha_1 \in R_{\langle 1 \rangle}$ 且 $a_1 < \alpha_1 < c$. 于是存在 $\alpha_i \in R_{\langle 1 \rangle}, i = 2, \dots, n$, 使得 $f(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$, 且 $-D < \alpha_i < D, i = 2, \dots, n$. 由赋值环 $A_{\langle n \rangle}$ 的结构, 有 $\alpha_i \in A_{\langle n \rangle}, i = 1, \dots, n$. 于是 $f(\pi(\alpha_1), \pi(\alpha_2), \dots, \pi(\alpha_n)) = \pi(f(\alpha_1, \alpha_2, \dots, \alpha_n)) = 0$ 即 $f(a_1, \pi(\alpha_2), \dots, \pi(\alpha_n)) = 0$. 这里 $\pi(\alpha_i) \in R, i = 2, \dots, n$. 从而有 $a_1 \in V_R(f, x_1)$, 矛盾. 由于 $V_R(f, x_j)$ 不是有界集, 从而它必有一个区间以 $+\infty$ 或 $-\infty$ 为端点. 如果 $+\infty$ 是 $V_R(f, x_j)$ 的某个区间的端点, 则必存在 $c \in R$, 使得 $c, +\infty (\subseteq V_R(f, x_j))$. 从而, 有如下语句在 R 中成立:

$$\forall x_j (x_j > c) \Rightarrow \exists (x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n) (f(x_1, x_2, \dots, x_n) = 0).$$

由转移定理, 上面语句在 $R_{\langle 1 \rangle}$ 中也成立. 注意到, $t^{-1} \in R_{\langle 1 \rangle}$ 且 $t^{-1} > c$, 从而存在 $\alpha_i \in R_{\langle 1 \rangle}, i = 1, \dots, j-1, j+1, \dots, n$, 使得 $f(\alpha_1, \dots, \alpha_{j-1}, t^{-1}, \alpha_{j+1}, \dots, \alpha_n) = 0$.

如果 $-\infty$ 为 $V_R(f, x_j)$ 的某个区间的端点, 则类似可证, 存在 $\alpha_i \in R_{\langle 1 \rangle}, i = 1, \dots, j-1, j+1, \dots, n$, 使得 $f(\alpha_1, \dots, \alpha_{j-1}, -t^{-1}, \alpha_{j+1}, \dots, \alpha_n) = 0$.

根据引理 1 和 2, 容易证明定理 1 和 2. 由于两定理可通过相同的方式加以证明, 仅证明定理 1.

定理 1 的证 必要性: 设方程 $f(X)=0$ 在 R 中有解. 当 $V_R(f, x_1)$ 无有限端点时, 必有 $V_R(f, x_1)=R$, 从而方程 $f(0, x_2, \dots, x_n)=0$ 在 R 中有解. 当 $V_R(f, x_1)$ 具有有限端点时, 根据引理 1 和 2, 叙述 (2) ~ (4) 之一成立.

充分性: 如果对于某个 $j \in \{2, \dots, n\}$, 方程 $f(x_1, \dots, x_{j-1}, t^{-1}, x_{j+1}, \dots, x_n)=0$ 或方程 $f(x_1, \dots, x_{j-1}, -t^{-1}, x_{j+1}, \dots, x_n)=0$ 在 $R_{\langle 1 \rangle}$ 中有解, 则下列语句在 $R_{\langle 1 \rangle}$ 中成立:

$$\exists (x_1, x_2, \dots, x_n)(f(x_1, x_2, \dots, x_n) = 0).$$

由于上面语句中的常量 (即多项式 $f(X)$ 的系数) 都在 R 中, 从而由转移定理, 上面语句在 R 中也成立, 即方程 $f(X)=0$ 在 R 中有解. 另外, 显然由叙述 (1) 或 (4) 可知, 方程 $f(X)=0$ 在 R 中有解.

当 $n=2$ 时, 由定理 1 和 2, 可以获得下面两个命题:

命题 1 设 $f(x, y) \in K[x, y]$, 则方程 $f(x, y)=0$ 在 R 中有解, 当且仅当如下 4 个叙述之一成立:

- (1) 方程 $f(0, y)=0$ 在 R 中有解;
- (2) 方程 $f(x, t^{-1})=0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (3) 方程 $f(x, -t^{-1})=0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (4) 方程组 $f(x, y)=0, \frac{\partial f(x, y)}{\partial y}=0$ 在 R 中有解.

命题 2 设 $f(x, y) \in K[x, y]$, 则方程 $f(x, y)=0$ 在 R 中有解, 当且仅当如下 4 个叙述之一成立:

- (1) 方程 $f(t^{-1}, y)=0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (2) 方程 $f(x, t^{-1})=0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (3) 方程 $f(x, -t^{-1})=0$ 在 $R_{\langle 1 \rangle}$ 中有解;
- (4) 方程组 $f(x, y)=0, \frac{\partial f(x, y)}{\partial y}=0$ 在 R 中有解.

将上面的结果与 Seidenberg 引理^[3] 相比较, 尽管增加了判别条件 (1) ~ (3), 但是用一个次数较低的多项式 $\frac{\partial f}{\partial y}$ 取代了 Seidenberg 引理中的 $x \frac{\partial f}{\partial y} - y \frac{\partial f}{\partial x}$, 这将给计算带来方便.

2 二元多项式的情形

本节将应用上面的结果给出一些有效算法, 用来判定 K 上一个二元多项式是否在 R 中有解 (等价于: 正定) 或者半定. 在下面讨论中, 将应用文献 [7] 中零维理想的正规化方法.

注意到: “去重因式” 不影响多项式的解集, “去偶次重因式” 不影响多项式的半定性, 同时这两种运算过程都是有效的, 且所产生的结果都是无重因式多项式. 因此, 在下文中, 不妨直接考虑无重因式的多项式.

引理 3 设 $f \in K[x, y]$ 无重因式, 且 $\alpha, \beta \in R_{\langle n \rangle}$, 使得 $f(\alpha, \beta)=0$. 如果 f 在 R 中是半定的, 则 $\alpha, \beta \in R$.

证 注意到半定的单元多项式必有重因式, 从而由条件知, 多项式 $f(x, y)$ 关于 x 和 y 的次数都大于零. 假设 $\alpha \notin R$ 或 $\beta \notin R$, 不失一般性, 不妨设 $\alpha \notin R$. 由于 R 在 $R_{\langle n \rangle}$ 中是代数闭的,

从而 α 是域 R 上的超越元. 由于 $f(\alpha, \beta) = 0$, 从而 β 是域 $K(\alpha)$ 上代数元. 令 $u(z)$ 是 β 在 $K(\alpha)$ 上的极小多项式. 由于 $K[\alpha]$ 是唯一分解整环, 从而 $u(z)$ 可表为 $u(z) = \gamma m(\alpha, z)$, 其中 $\gamma \in K(\alpha)$, $m(\alpha, z) \in K[\alpha][z]$ 是 $K[\alpha]$ 上的一个含 z 的本原多项式.

由条件, 可设 f 是半正定的而不失一般性. 由半正定多项式的表示 (见文献 [10] 中定理 7.2), f 可表示为

$$f = \sum_{i=1}^s a_i \left(g_i / h \right)^2,$$

其中 $0 < a_i \in K$, $h, g_i \in K[x, y]$ 且 $h \neq 0$, $i = 1, \dots, s$.

从而, 进一步有

$$h^2 f = \sum_{i=1}^s a_i g_i^2.$$

在众多的如上表达式中, 选取这样的等式, 其中 h 具有极小(全)次数. 由此有 $\sum_{i=1}^s a_i g_i^2(\alpha, \beta) = h^2(\alpha, \beta) f(\alpha, \beta) = 0$, 从而必有 $g_i(\alpha, \beta) = 0$, $i = 1, \dots, s$. 于是在 $K(\alpha)[z]$ 中, $u(z) \mid g_i(\alpha, z)$, 自然有 $m(\alpha, z) \mid g_i(\alpha, z)$, $i = 1, \dots, s$. 由 $m(\alpha, z)$ 的本原性, 从而在 $K[\alpha, z]$ 中, $m(\alpha, z) \mid g_i(\alpha, z)$, $i = 1, \dots, s$. 由于 α, z 是 K 上无关的超越元, 从而 $m(x, y) \mid g_i$, $i = 1, \dots, s$. 因而, $m^2(x, y) \mid \sum_{i=1}^s a_i g_i^2$, 即 $m^2(x, y) \mid h^2 f$. 由于 f 无重因式, 从而有 $m(x, y) \mid h^2$. 注意到 $m(x, y)$ 是 $K[x, y]$ 中不可约多项式, 从而有 $m(x, y) \mid h$. 令 $h = m(x, y) h_1$, $g_i = m(x, y) g_{i1}$, $i = 1, \dots, s$, 则由上面的关系式, 可化得

$$h_1^2 f = \sum_{i=1}^s a_i g_{i1}^2,$$

这里, h_1 的次数小于 h 的次数, 与选取矛盾.

引理 4 设 $f \in K[x, y]$ 无重因式, 则 f 在 R 中是半定的, 当且仅当 f 在 R^2 中只有有限个零点.

证 充分性: 设 $f(x, y)$ 在 R 中不是半定的, 则存在 $(a, b), (c, d) \in R^2$, 使得 $f(a, b) > 0$, 而 $f(c, d) < 0$. 不失一般性, 设 $a \neq c$. 由多项式函数的连续性, 存在 d 的开邻域 S , 使得 $f(c, \xi) < 0$, $\forall \xi \in S$. 对于每个 $\xi \in S$, 作单元多项式 $\Psi(z) \doteq f(a + z(c - a), b + z(\xi - b))$, 则 $\Psi(0)\Psi(1) = f(a, b)f(c, \xi) < 0$. 由中间值定理, 存在 $\lambda_\xi \in (0, 1)$, 使得 $f(a + \lambda_\xi(c - a), b + \lambda_\xi(\xi - b)) = 0$. 于是 $f(x, y)$ 有无穷多个相异的零点 $(a + \lambda_\xi(c - a), b + \lambda_\xi(\xi - b))$, $\xi \in S$.

必要性: 设 f 在 R^2 中有无限多个零点, 则 $V_R(f, x)$ 或 $V_R(f, y)$ 至少有一个是无限集. 不妨设 $V_R(f, x)$ 是无限集. 这样, 除包含有限个点外, $V_R(f, x)$ 还包含至少一个(左右端点不相同的)区间. 于是有 $a, b (\subseteq V_R(f, x))$, 这里 $a, b \in R$ 且 $a < b$. 从而, 如下语句在 R 中成立:

$$\forall x (a < x < b) \Rightarrow \exists y (f(x, y) = 0).$$

由转移定理, 上面语句在 $R_{(1)}$ 中也成立. 令 $\alpha = a + t$, 则 $\alpha \in R_{(1)}$ 且 $a < \alpha < b$. 从而存在 $\beta \in R_{(1)}$, 使得 $f(\alpha, \beta) = 0$. 此时, 显然 $\alpha \notin R$. 由引理 3 知, $f(x, y)$ 不是半定的. 证毕.

对于 $K[x, y]$ 中一个无重因式多项式 $f(x, y)$, 总可通过“求最大公因式”的有效方法, 将 $f(x, y)$ 表为 $f(x, y) = h(x)g(x, y)$, 其中 $h(x) \in K[x]$, $g(x, y) \in K[x, y]$, 且 $g(x, y)$ 是在 $K[x]$ 上含 y 的本原多项式(即 x -本原多项式). 显然, $f(x, y)$ 有实零点, 当且仅当 $h(x)$ 有实

零点或 $g(x, y)$ 有实零点. 同时, 由引理 4 易知, $f(x, y)$ 是半定的, 当且仅当 $h(x)$ 在 R 中无零点且 $g(x, y)$ 是半定的. 因此, 只需考虑无重因式的 x -本原多项式.

设 $f(x, y)$ 是 $K[x, y]$ 中一个无重因式的 x -本原多项式, $g = \frac{\partial f(x, y)}{\partial y}$, 且用 (f, g) 表示 $K[x, y]$ 中由 f, g 生成的理想. 令 $\text{Res}(f, g, x)$, $\text{Res}(f, g, y)$ 分别是 f 和 g 关于 x, y 的结式. 由结式的一个熟知结果^[3], $\text{Res}(f, g, x), \text{Res}(f, g, y) \in (f, g)$. 假若 $\text{Res}(f, g, x) = 0$, 则 f 和 g 有非常量公因式, 从而有公共的不可约因式 p . 由于 $f(x, y)$ 是 x -本原的, 从而 p 中必含变元 y . 又由于 g 是 f 关于变量 y 的偏导数, 从而 p 是 f 的重因式, 矛盾. 同样可证, $\text{Res}(f, g, y) \neq 0$. 又设 $u(x), v(y)$ 分别是 $\text{Res}(f, g, y), \text{Res}(f, g, x)$ 的无重因式部分. 由文献[7]中引理 8.13 易知, $(f, g, u(x), v(y))$ 是 $K[x, y]$ 中一个维数 ≤ 0 的根理想, 并且 $(f, g, u(x), v(y))$ 的维数为零, 当且仅当 $u(x)$ 和 $v(y)$ 都不是 K 中常量.

现设 $u(x) \notin K$ 且 $v(y) \notin K$, 即根理想 $(f, g, u(x), v(y))$ 的维数 $= 0$. 由文献[7]中命题 8.77 和定理 8.81 知, 通过有限次测试, 必可获得某个 $e \in K$ (甚至可取 e 为整数), 使得通过变换: $x \rightarrow x, y \rightarrow y - ex$ 后, 理想 $(f, g, u(x), v(y))$ 处于正规位置, 且其关于字典序 $y \ll x$ 的简化 Gröbner 基具有如下形式:

$$\{x - w(y), \phi(y)\},$$

这里 $w(y), \phi(y) \in K[y]$.

定理 3 设 $f(x, y), g(x, y), u(x)$ 和 $v(y)$ 同上, 则方程 $f(x, y) = 0$ 在 R 中有解, 当且仅当下面 4 个叙述之一成立:

- (1) 一元方程 $f(0, y) = 0$ 在 R 中有解;
- (2) 一元方程 $f(x, t^{-1})$ 在 $R_{(1)}$ 中有解;
- (3) 一元方程 $f(x, -t^{-1})$ 在 $R_{(1)}$ 中有解;
- (4) $u(x), v(y) \notin K$, 且一元方程 $\phi(y) = 0$ 在 R 中有解, 这里 $\phi(y)$ 同上.

证 只需证明, 命题 1 中叙述(4)等价于定理中叙述(4). 由结式的另一个熟知事实知, (f, g) 和 $(f, g, u(x), v(y))$ 在 R 中有相同的零点集. 再由 Gröbner 基的定义, 显然 $(f, g, u(x), v(y))$ 在 R 中的零点集与 $(x - w(y), \phi(y))$ 在 R 中的零点集是一一对应的, 而后者由方程 $\phi(y) = 0$ 在 R 中的解唯一决定.

注 在上面的讨论中, 若 $\text{Res}(f, g, x)$ 和 $\text{Res}(f, g, y)$ 都无重因式, 则 $(f, g) = (f, g, u(x), v(y))$, 从而 (f, g) 是 $K[x, y]$ 中维数 ≤ 0 的根理想.

作为定理 3 的一个应用, 给出下面的例子.

例 1 确定方程 $f(x, y) = 0$ 是否有实解, 这里 $f(x, y) = x^2 y^2 + x^2 - xy + y^4 - y^2 + 1$.

计算过程: (1) 考虑多项式 $f(0, y) = y^4 - y^2 + 1$, 易知它无实零点.

(2) 考虑多项式 $f(x, t^{-1}) = (1 + t^{-2})x^2 - t^{-1}x + (t^{-4} - t^{-2} + 1)$. 这是一元二次多项式, 其判别式 $\Delta = (-t^{-1})^2 - 4(1 + t^{-2})(t^{-4} - t^{-2} + 1)$. 注意到, Δ 作为含 t^{-1} 的多项式, 其首项系数为 -4 , 且 t^{-1} 在有理数域上是无限大正元素. 从而 $\Delta < 0$. 因此, $f(x, t^{-1})$ 无实零点.

(3) 类似于过程(2)可知, $f(x, -t^{-1})$ 无实零点.

(4) 计算 $g = \frac{\partial f}{\partial y} = 2x^2 y - x + 4y^3 - 2y$. 经检验, $\text{Res}(f, g, x)$ 和 $\text{Res}(f, g, y)$ 都无重因式.

通过正规化变换: $x \rightarrow x$, $y \rightarrow y - 0x$, 理想 (f, g) 关于字典序 $y \ll x$ 的简化 Gröbner 基为

$$\{2x - 4y^9 - 20y^7 - 23y^5 + 17y^3 + 9y, 4y^{10} + 16y^8 + 3y^6 - 36y^4 + 16y^2 + 1\}.$$

借助于 Sturm 定理的判定可知, 多项式 $4y^{10} + 16y^8 + 3y^6 - 36y^4 + 16y^2 + 1$ 无实根.

根据定理 3, 所给的多项式方程 $f(x, y) = 0$ 无实解. 换句话说, $f(x, y)$ 是(正)定的.

至于多项式半定性的判定, 下面简单的引理表明: 可将问题转化为判定解的存在性.

引理 5 设 $f(X) \in K[x_1, \dots, x_n]$, 且它关于某一字典序的首项系数的符号为 $\epsilon (= \pm 1)$, 则 $f(X)$ 在 R 中半定, 当且仅当 $f(X) + \epsilon\eta$ 在 $R_{\langle n \rangle}^n$ 中无零点, 这里 $\eta \in R_{\langle n \rangle}$ 是 K 上的正无限小元素.

证 必要性: 假若 $f(X) + \epsilon\eta$ 有零点 $\alpha^* \in R_{\langle n \rangle}^n$, 则 $f(\alpha^*) + \epsilon\eta = 0$. 由此有 $\epsilon f(\alpha^*) = -\epsilon^2\eta < 0$. 由转移定理存在 $\alpha \in R^n$, 使得 $\epsilon f(\alpha) < 0$. 注意到 $\epsilon f(X)$ 的首项系数为正, 从而必存在 $\beta \in R^n$, 使得 $\epsilon f(\beta) > 0$. 这表明 $f(X)$ 在 R 中不是半定的.

充分性: 假若 $f(X)$ 在 R 中不是半定的, 则存在 $\alpha, \beta \in R^n$, 使得 $f(\alpha) > 0$, 但 $f(\beta) < 0$. 从而有 $f(\alpha) + \epsilon\eta > 0$, 但 $f(\beta) + \epsilon\eta < 0$. 由实闭域 $R_{\langle n \rangle}$ 上的中间值定理, $f(X) + \epsilon\eta$ 在 $R_{\langle n \rangle}^n$ 中有零点.

由引理 5, 容易建立

定理 4 设 $f(x, y)$ 同定理 3, 且 ϵ 是 $f(x, y)$ 关于某个字典序的首项系数的符号, 则 $f(x, y)$ 在 R 中半定, 当且仅当下面 4 个叙述都成立:

- (1) $f(0, y)$ 在 R 中的每个根具有偶重数(即 $f(0, y)$ 在 R 中是半定的);
- (2) 方程 $f(x, t^{-1}) = 0$ 在 $R_{\langle 1 \rangle}$ 中无解;
- (3) 方程 $f(x, -t^{-1}) = 0$ 在 $R_{\langle 1 \rangle}$ 中无解;
- (4) 方程组 $f(x, y) + \epsilon t = 0, \frac{\partial f(x, y)}{\partial y}$ 在 $R_{\langle 1 \rangle}$ 中无解.

证 记 $f_1(x, y) \doteq f(x, y) + \epsilon t \in K_{\langle 1 \rangle}[x, y]$.

必要性: 设 $f(x, y)$ 在 R 中是半定的. 显然, $f(0, y)$ 在 R 中也是半定, 从而有叙述(1). 再由引理 3, 易得叙述(2)和(3). 此外, 由引理 5 知, $f_1(x, y)$ 在 $R_{\langle 1 \rangle}$ 中无零点, 从而叙述(4)显然成立.

充分性: 为简便起见, 不妨设 $\epsilon = +1$. 由转移定理和叙述(2)可知, $f(x, t^{-1})$ 在 $R_{\langle n \rangle}$ 中也无零点. 注意到子域 $K(t_2)$ 序同构于 $K(t)$, 从而可知, $f(x, t_2^{-1})$ 在 $R_{\langle n \rangle}$ 中无零点. 于是 $f(t_2^{-1}, t^{-1})$ 与 $f(1, t^{-1})$ 同号, 而 $f(t^{-1}, t_2^{-1})$ 与 $f(1, t_2^{-1})$ 同号. 由于 $f(1, t^{-1})$ 与 $f(1, t_2^{-1})$ 同号, 从而 $f(t_2^{-1}, t^{-1})$ 与 $f(t^{-1}, t_2^{-1})$ 有相同符号. 由 $K_{\langle n \rangle}$ 的序结构知, $f(t_2^{-1}, t^{-1})$ 和 $f(t^{-1}, t_2^{-1})$ 中总有一个的符号为 $\epsilon = +1$. 从而可知 $f(x, t^{-1})$ 和 $f(x, t_2^{-1})$ 都是正定的. 于是 $f(x, t_2^{-1}) + t$ 即 $f_1(x, t_2^{-1})$ 在 $R_{\langle 2 \rangle}$ 中无零点.

由(1)知, $f(0, y)$ 在 R 中是半定的. 由上面讨论, $f(x, t^{-1})$ 是正定的, 从而 $f(0, t^{-1}) > 0$. 于是 $f(0, y)$ 是半正定的. 从而 $f(0, y) + t$ 即 $f_1(0, y)$ 在 $R_{\langle 1 \rangle}$ 中无零点.

又由于 $f(0, y)$ 是半正定的, 从而 $f(0, -t^{-1}) \geq 0$. 再由叙述(3)即知, $f(x, -t^{-1})$ 是正定的. 同样, 由此可得 $f(x, -t_2^{-1})$ 也是正定的. 从而 $f(x, -t_2^{-1}) + t$ 即 $f_1(x, -t_2^{-1})$ 在 $R_{\langle 2 \rangle}$ 中无零点.

再由叙述(4), 方程组 $f_1(x, y) = 0, \frac{\partial f_1(x, y)}{\partial y} = 0$ 在 $R_{(1)}$ 中无解. 注意到 t_2 是 $K_{(1)}$ 上的无限小正元素. 根据命题 1, 方程 $f_1(x, y) = 0$ 在 $R_{(1)}$ 中无解. 最后由引理 5, $f(x, y)$ 在 R 中是半定的.

作为定理 4 的一个应用, 给出下面的例子. 为叙述方便, 约定: 对于一个含变量 x 的非零单元多项式 $f(x)$, 用 $f(+\infty)$ 表示 $f(x)$ 的首项系数, 且 $f(-\infty) = (-1)^d f(+\infty)$, 这里 d 为 $f(x)$ 的次数. 此外, 对于一个非零多项式 $f(x, y) \in K[x, y]$, 可以在 $K(y)[x]$ 中计算 $f(x, y)$ 关于变量 x 的 Sturm 序列. 一般说来, 这序列中某些成员是分母在 $K[y]$ 中的有理表达式. 为去掉这些表达式中的分母, 可用各自分母的平方乘上这些表达式, 从而得到 $K[x, y]$ 中一个新序列. 在下文中, 这样一个新序列称作 $f(x, y)$ 关于 x 的一个修正 Sturm 序列.

例 2 确定多项式 $f(x, y)$ 是否半定, 这里 $f(x, y) = x^4 + x^2 y^2 + 2y^4 - 4xy + 1$.

计算过程: (1) 考虑多项式 $f(0, y) = 2y^4 + 1$, 易知它无实零点.

(2) 计算多项式 $f(x, y)$ 关于变量 x 的一个修正 Sturm 序列如下:

$$f_1 = f, \quad f_2 = \frac{\partial f}{\partial x}, \quad f_3 = -x^2 y^2 + 6xy - 4y^4 - 2,$$

$$f_4 = y^2(7y^4 - 68)x + 2y(25y^4 + 12), \quad f_5 = 98y^{12} + 445y^8 - 200y^4 + 16.$$

从而,

$$f_1(+\infty, t^{-1}) = 1 > 0, \quad f_2(+\infty, t^{-1}) = 4 > 0, \quad f_3(+\infty, t^{-1}) = -t^{-2} < 0,$$

$$f_4(+\infty, t^{-1}) = t^{-2}(7t^{-4} - 68) > 0, \quad f_5(+\infty, t^{-1}) = 98t^{-12} + 445t^{-8} - 200t^{-4} + 16 > 0.$$

相应的符号差为 2.

通过类似的计算知, 序列 $f_1(-\infty, t^{-1}), f_2(-\infty, t^{-1}), f_3(-\infty, t^{-1}), f_4(-\infty, t^{-1}), f_5(-\infty, t^{-1})$ 的符号差也为 2.

由 Sturm 定理知, $f(x, t^{-1})$ 无实零点.

(3) 类似于过程(2)可知, $f(x, -t^{-1})$ 无实零点.

(4) 令 $g \doteq \frac{\partial f}{\partial y}$. 经检验, $\text{Res}(f+t, g, x)$ 和 $\text{Res}(f+t, g, y)$ 都无重因式. 计算理想 $(f+t, g)$ 关于字典序 $y \ll x$ 的简化 Gröbner 基为

$$\{(72t - 632)x + 1764y^{11} + (4132 + 252t)y^7 + (861 - 538t + 9t^2)y^3, \\ 196y^{12} + (372 + 28t)y^8 + (t^2 - 66t - 163)y^4 + 16 + 16t\}.$$

这表明: 理想 $(f+t, g)$ 关于变量 y 处于正规位置. 从而方程组 $f+t=0, g=0$ 有实解, 当且仅当多项式 $196y^{12} + (372+28t)y^8 + (t^2-66t-163)y^4 + 16+16t$ 有实零点. 显然, 这又相当于下面多项式 h 有非负的实零点:

$$h \doteq 196z^3 + (372 + 28t)z^2 + (t^2 - 66t - 163)z + 16 + 16t.$$

计算多项式 h 关于变量 z 的修正 Sturm 序列如下:

$$h_1 = h, \quad h_2 = \frac{\partial h}{\partial z}, \quad h_3 = (117114 + 29820t + 98t^2)z + 7t^3 - 369t^2 - 14335t - 22215,$$

$$h_4 = 1391743 - 30947934t - 2470358t^2 + 1847000t^3 - 142785t^4 + 1134t^5.$$

从而, $h_1(+\infty) = 196 > 0, h_2(+\infty) = 58 > 0, h_3(+\infty) = 117114 + 29820t + 98t^2 > 0, h_4(+\infty) =$

$h_4 > 0$. 相应的符号差为 0.

而 $h_1(0) = 16 + 16t > 0$, $h_2(0) = -162 - 66t + t^2 < 0$, $h_3(0) = 7t^3 - 369t^2 - 14\,335t - 22\,215 < 0$, $h_4(0) = h_4 > 0$. 相应的符号差为 2.

由 Sturm 定理可知, 多项式 h 有正的实根. 从而, 方程组 $f+t=0$, $g=0$ 有实解.

根据定理 4, 所给的多项式 $f(x, y)$ 是不定的.

最后, 给出半定二元多项式的又一判定方法. 对于一个非零多项式 $f(x) \in K[x]$, K 的一个有限子集 Γ 称为 $f(x)$ 在 K 中的一个隔离集. 如果下列条件满足: (1) 对于每个 $a \in \Gamma$, $f(a) \neq 0$; (2) 对于每个 $f(x)$ 在 R 中的零点 α , 总存在 $a, b \in \Gamma$, 使得 $a < b$, 且开区间 $]a, b[$ 恰好只包含 $f(x)$ 的这个零点 α . 在下文中, 总假定序域 $(K, \leq)$ 容许一个有效方法, 使得对于每个非零多项式 $f(x) \in K[x]$, 可计算 $f(x)$ 在 K 中的一个隔离集. 由文献[7]中定理 8.115 知, 当 $K=Q$ 时, 这样一个有效的方法可得到.

设 $f(x, y)$ 是 $K[x, y]$ 中一个无重因式的 x -本原多项式, 且 $g \doteq \frac{\partial f}{\partial y}$. 由前面的讨论知, $\text{Res}(f, g, y) \neq 0$. 此时, 可以建立

定理 5 设 $f(x, y)$ 和 $g(x, y)$ 同上, 且 Γ 为 $\text{Res}(f, g, y)$ 在 K 中的一个隔离集, 则 $f(x, y)$ 在 R 中半定, 当且仅当下面叙述都成立:

- (1) 一元方程 $f(t^{-1}, y) = 0$ 在 $R_{(1)}$ 中无解;
- (2) 一元方程 $f(x, t^{-1}) = 0$ 在 $R_{(1)}$ 中无解;
- (3) 一元方程 $f(x, -t^{-1}) = 0$ 在 $R_{(1)}$ 中无解;
- (4) 对于每个 $a \in \Gamma$, 方程 $f(a, y) = 0$ 在 R 中无解.

证 必要性: 设 $f(x, y)$ 在 R 中半定. 由引理 3, 可得叙述 (1) ~ (3). 由引理 4, f 在 R^2 中只有有限个零点, 从而 $V_R(f, x)$ 是由有限个点 (即左右端点都相同的区间) 组成的. 因此, $V_R(f, x)$ 中每个点都是闭端点. 对于每个 $\alpha \in V_R(f, x)$, 存在 $\beta \in V_R(f, y)$, 使得 $f(\alpha, \beta) = 0$. 由引理 1 知, $g(\alpha, \beta) = 0$. 从而 α 是结式 $\text{Res}(f, g, y)$ 在 R 中的零点. 这说明, $V_R(f, x) \cap \Gamma = \emptyset$. 于是, 对于每个 $a \in \Gamma$, $f(a, y)$ 在 R 中无零点.

充分性: 由叙述 (1) 知, $V_R(f, x) \neq R$. 再由叙述 (2) 和 (3) 以及引理 2 知, $V_R(f, x)$ 无开的有限端点. 于是 $V_R(f, x)$ 的每个有限端点都是闭的. 设 Π 是 $V_R(f, x)$ 的任一区间, 则 $\Pi \neq R$, 从而 Π 有一个有限闭端点 α . 由必要性的证明知, α 是 $\text{Res}(f, g, y)$ 在 R 中的一个零点. 于是, 存在 $a, b \in \Gamma$, 使得 $a < b$, 且开区间 $]a, b[$ 恰好只包含 $f(x)$ 的这个零点 α . 如若 $\Pi \neq]\alpha, \alpha[$, 则易知, $a \in \Pi$ 或 $b \in \Pi$. 由于 $\Pi \subseteq V_R(f, x)$, 从而方程 $f(a, y) = 0$ 或 $f(b, y) = 0$ 在 R 中有解, 与叙述 (4) 矛盾. 于是 $\Pi =]\alpha, \alpha[$. 这说明, $V_R(f, x)$ 仅由有限个点组成. 假若 $V_R(f, y)$ 有无限多个元素, 则由抽屉原理, 存在某个 $\alpha \in V_R(f, x)$ 以及 $V_R(f, y)$ 的某个无限子集 B , 使得 $f(\alpha, \beta) = 0, \forall \beta \in B$. 于是多项式 $f(\alpha, y) \equiv 0$. 从而在 $R[x, y]$ 中有 $(x - \alpha) \mid f(x, y)$, 与 $f(x, y)$ 的 x -本原性矛盾. 因而, $V_R(f, y)$ 只有有限个点. 这样, $f(x, y)$ 在 R^2 中只有有限个零点. 由引理 4 知, $f(x, y)$ 是半定的.

作为定理 5 的一个应用, 给出下面的例, 这一例子曾在文献[4, 12] 中以不同的方式讨论过.

例 3 确定多项式 $f(x, y)$ 是否半定, 这里 $f(x, y) = x^6 - x^4y^2 - x^2y^4 + y^6 - x^4 + 3x^2y^2 -$

$$y^4 - x^2 - y^2 + 1.$$

计算过程: 计算 f 和 $\frac{\partial f}{\partial y}$ 关于 y 的结式得 $\text{Res}(f, g, y) = 64(x^2 + 1)(x - 1)^6(x + 1)^6x^4(32x^4 - 61x^2 + 32)^2$. 容易知道, 点集 $\Gamma = \{-2, -1/2, 1/2, 2\}$ 是 $\text{Res}(f, g, y)$ 在 $\mathbb{Q}$ 中的一个隔离集.

注意到 $f(x, y)$ 是对称的, 根据定理 5, 只需指明: 对于每个 $a \in \Gamma \cup \{t^{-1}, -t^{-1}\}$, $f(a, y)$ 是否有实零点. 令 $h(x, z) \doteq x^6 - x^4z - x^2z^2 + z^3 - x^4 + 3x^2z - z^2 - x^2 - z + 1$. 显然, 这又相当于: 对于每个 $a \in \Gamma \cup \{t^{-1}, -t^{-1}\}$, 确定多项式 $h(a, z)$ 是否有非负的实零点.

借助于 Sturm 定理, 通过类似的计算可知, 对于每个 $a \in \Gamma \cup \{t^{-1}, -t^{-1}\}$, 多项式 $h(a, z)$ 无非负的实零点. 根据定理 5, 所给的多项式 $f(x, y)$ 是半(正)定的.

致谢 感谢广州师范学院梁松新博士赠送 Maple V Release 4 光盘.

参 考 文 献

- 1 吴文俊. 几何定理机器证明的基本原理. 北京: 科学出版社, 1984. 208 ~ 228
- 2 Tarski K. A Decision Method for Elementary Algebra and Geometry. Berkeley: Rand Corporation, 1951
- 3 Seidenberg A. A new decision method for elementary algebra. Ann Math, 1954 60(2): 365 ~ 374
- 4 杨 路, 侯晓荣, 曾振柄. 多项式的完全判别系统. 中国科学, E 辑, 1996, 26(5): 424 ~ 441
- 5 杨 路, 张景中, 侯晓荣. 非线性代数方程组与定理机器证明. 上海: 上海科技教育出版社, 1996
- 6 Heck A. Introduction to Maple. New York: Springer-Verlag, 1993
- 7 Becker T, Weispfenning V, Kredel H. Gröbner Bases: A Computational Approach to Commutative Algebra. New York: Springer-Verlag, 1993
- 8 Prestel A. Lectures on Formally Real Fields. Lecture Notes in Math, Vol 1 093, Berlin: Springer-Verlag 1984
- 9 Knebusch M. On the extension of real places. Comment Math Helv 1973, 48(3): 354 ~ 369
- 10 Lam T Y. The Theory of Ordered Fields. Lecture Notes in Pure and Appl Math, 55. New York: M Dekker, 1980. 1 ~ 152
- 11 Bochnack J, Coste M, Roy M F. Géométrie Algébrique Réelle. New York: Springer-Verlag 1987
- 12 梁松新, 李传中. 有理数域上二元多项式半正定性的判定. 计算机应用, 1998, 18(3): 28 ~ 29