系 统 科 学 与 数 学
J. Sys. Sci. & Math. Scis.
31(8) (2011, 8), 903-912

代数数极小多项式的近似重构*

陈 经 纬 冯 勇 秦 小 林 张 景 中

(中国科学院重庆绿色智能技术研究院, 重庆 401122; 中科院成都计算机应用研究所, 成都 610041;
中国科学院研究生院, 北京 100049)

摘要 给出了代数数极小多项式近似重构的误差控制条件, 进而基于同步整数关系探测算法 SIRD, 得到一个从代数数近似值重构其准确极小多项式的完备的新算法, 从而将 "采用近似计算获得准确值" 这一思想的适用范围从有理数扩展到代数数.

关键词 同步整数关系, 代数数, 极小多项式.

MR(2000) 主题分类号 33F10, 68W30

1 引 言

求解单变元多项式方程是数学领域中一个古老、基本而内容丰富的问题. 著名的代数学基本定理告诉我们任意一个 n 次复系数单变元多项式有一个复根, 而 Galois 理论则指出次数大于等于 5 的代数方程没有根式解. 因此在实际应用中, 求解单变元多项式方程主要利用数值方法 (如 Newton 迭代法) 求得近似解. 本文主要研究这一问题的逆问题, 即给定一个近似值, 找出一个准确的一元多项式, 使得给定的近似值恰好对应到该多项式的某个准确根.

称 α 为一个 代数数, 如果存在 $P(x) \in \mathbb{Z}[x]$ 使得 $P(\alpha) = 0$. 称 $P(x)$ 为代数数 α 的 极小多项式, 如果 $P(x)$ 是 $\mathbb{Z}[x]$ 中满足 $P(\alpha) = 0$ 的次数最低的本原多项式. 代数数 α 的 次数定义作其极小多项式的次数. 代数数 α 的 高度 height(α) 定义为其极小多项式 $P(x)$ 的 高度 height(P), 即 $P(x)$ 系数绝对值的最大值. 现将本文所讨论的问题作如下精确描述.

问题 1 设一未知代数数 α 的次数不超过 n, 高度不超过 H. 能否从某一精度的近似值 $\overline{\alpha}$ 推断出 α 准确的极小多项式?

该问题最早由著名的理论计算机科学家, 1995 年 Turing 奖获得者 Manuel Blum 于 20 世纪 80 年代在研究伪随机序列时提出 (见 [1]).

当 $n = 1$ 时, 即有理数的近似重构, 可以通过 Euclid 算法 [2] 或者连分数算法 [3] 予以解决.

* 国家 973 计划资助 (2011CB302400), 国家自然科学基金资助 (10771205), 中国科学院知识创新基金 (KJCX2-YW-S02) 资助和中国科学院西部之光项目资助.

通讯作者: yongfeng@casit.ac.cn

收稿日期: 2010-11-02.

当 $n>1$ 时， Kannan, Lenstra 和 Lovász 于 1984 年利用著名的 LLL 算法 [4] 给出了第一个肯定回答 [1]. 随着 LLL 算法在计算机科学中的广泛应用，其改进和推广也不断涌现，如 [5–7] 等. 相应地，基于 LLL 的极小多项式重构算法也得到改进，较新的进展可以参见文献 [8].

事实上,对于实代数数,通过整数关系探测也可以解决该问题 [9]. 设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)^{\mathrm{T}}\in\mathbb{R}^n$ (本文所涉向量均为列向量,用黑体字母表示). 称 $\boldsymbol{m}=(m_1,m_2,\cdots,m_n)^{\mathrm{T}}\in\mathbb{Z}^n\backslash\{\boldsymbol{0}\}$ 为 $\boldsymbol{x}$ 的一个整数关系, 如果 $\langle\boldsymbol{m},\boldsymbol{x}\rangle=m_1x_1+m_2x_2+\cdots+m_nx_n=0$. 为了得到 n 次代数数 α 的极小多项式，文 [9] 中通过整数关系探测算法 PSLQ[10] 寻找 $(1,\alpha,\cdots,\alpha^n)^{\mathrm{T}}$ 的一个整数关系. 然而对于复代数数的情形， PSLQ 算法便无能为力了. 因为对一个复数向量， PSLQ 仅仅能找到一组 Gauss 整数关系 [10–11]. 本文作者近期得到了一个同步整数关系探测的新算法 SIRD[11]. 该算法能有效地找到一个非零整数向量使其同时成为 t $(1\le t\le n-1)$ 个已知实数向量的整数关系. 对一个 n 次复代数数 α, 记 $\boldsymbol{x}_1=(1,\mathrm{Re}(\alpha),\cdots,\mathrm{Re}(\alpha^n))^{\mathrm{T}}$ 和 $\boldsymbol{x}_2=(0,\mathrm{Im}(\alpha),\cdots,\mathrm{Im}(\alpha^n))^{\mathrm{T}}$. 对 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 应用同步整数关系探测算法 SIRD 可以得到一个整数向量 $\boldsymbol{p}\in\mathbb{Z}^{n+1}$ 使得 $\langle\boldsymbol{p},\boldsymbol{x}_1\rangle=\langle\boldsymbol{p},\boldsymbol{x}_2\rangle=0$, 从而得到 α 的极小多项式.

本文采用上述策略，得到一个解决问题 1 的完备方法. 因为整数关系探测是基于推广的 Euclid 算法 [12], 所以本文的方法与已有基于 LLL 格约化的算法 [1,8] 是不同的. 然而要从 α 的近似值推断出其准确的极小多项式，必须对该近似值的误差进行控制，才能使得到的结果准确可信.

设 α 为一个高度不超过 H 的 n 次复代数数，其近似值 $\overline{\alpha}$ 满足

$$\max_{1\le i\le n}|\alpha^i-\overline{\alpha}^i|\le\varepsilon. \tag{1}$$

为了从近似值 $\overline{\alpha}$ 推断出 α 的精确的极小多项式, 可以利用 SIRD 算法寻找 $\boldsymbol{x}_1=(1,\mathrm{Re}(\overline{\alpha}),\cdots,\mathrm{Re}(\overline{\alpha}^n))^{\mathrm{T}}$ 和 $\boldsymbol{x}_2=(0,\mathrm{Im}(\overline{\alpha}),\cdots,\mathrm{Im}(\overline{\alpha}^n))^{\mathrm{T}}$ 的一个同步整数关系 $\boldsymbol{p}=(p_0,p_1,\cdots,p_n)^{\mathrm{T}}\in\mathbb{Z}^{n+1}$ 使得 $\langle\boldsymbol{p},\boldsymbol{x}_1\rangle=\langle\boldsymbol{p},\boldsymbol{x}_2\rangle=0$. 令 $p(x)=\sum\limits_{i=0}^{n}p_ix^i$, 则 $p(\overline{\alpha})=0$. 尽管由于计算机不能精确地实现实数操作，得到的整数关系不一定满足 $p(\overline{\alpha})=0$, 但总可以保证 $|p(\overline{\alpha})|$ 很小. 本文证明了如下定理.

定理 1 记号同上. 设多项式 $p(x)=\sum\limits_{i=0}^{n}p_ix^i\in\mathbb{Z}[X]$ 的高度 $\mathrm{height}(p)\le H$. 若

$$\varepsilon<\frac{1}{2}(n+1)^{-\frac{3}{2}n}H^{-2n}, \tag{2}$$

则

$$p(\alpha)=0\ \Leftrightarrow\ |p(\overline{\alpha})|<\frac{1}{2}(n+1)^{-\frac{3}{2}n+1}H^{-2n+1}. \tag{3}$$

定理 1 指出在满足一定的误差控制条件下 (见式 (8)), 可以通过近似值获得代数数准确的极小多项式. 这在某种意义上也意味着在此误差控制下，从代数数的近似值可以得出其准确值，从而将 Zhang 和 Feng 在 [3] 中提出的 “采用近似计算获得准确值” 这一思想的适用范围从有理数扩展到所有的代数数. 而且本文的误差控制是向下兼容的，即该误差控制不仅

适合于虚代数数，也适用于实代数数. 特别地，当 α 为有理数时，$n=1$, 相应的误差控制为 $|\alpha-\overline{\alpha}|<\frac{1}{\sqrt{2}H^2}$, 优于 [3] 中的误差控制 $|\alpha-\overline{\alpha}|<\frac{1}{2H^2}$.

根据 (8) 的误差控制，基于同步整数关系探测算法 (SIRD), 本文给出一个代数数极小多项式近似重构的新算法，该算法是完备的，确定的；并在计算机代数系统 Maple 中实现了该算法；通过理论分析、实例研究和与已有算法的比较，可以发现本文的结果具有以下几个方面的特点：

1) 相对于 [9] 中方法而言，本文的算法是完备的，完整地解决了问题 1;

2) 误差控制条件优于已有相应的误差控制；

3) 在满足该误差控制的条件下，本文的算法能确保输出是该代数数准确值的极小多项式；

4) 针对较大规模的问题，使用本文的算法有较好的效果.

以下各节内容安排如下. 第 2 节简要介绍同步整数关系探测算法 SIRD 及其性质；第 3 节研究误差控制并得到一个基于整数关系探测的代数数极小多项式近似重构的新算法；第 4 节通过实例讨论本文算法的特点和应用.

2　同步整数关系探测

定义 1　设 $\boldsymbol{x}_i=(x_{i,1},x_{i,2},\cdots,x_{i,n})^{\mathrm{T}}\in\mathbb{R}^n, i=1,2$. 若存在非零整数向量 $\boldsymbol{m}=(m_1,m_2,\cdots,m_n)^{\mathrm{T}}$ 使得 $\sum\limits_{j=1}^{n}m_jx_{i,j}=0$, 则称 $\boldsymbol{m}$ 为 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 的同步整数关系.

本文假设 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 是线性无关的，且满足

$$\begin{vmatrix} x_{1,n-1} & x_{2,n-1} \\ x_{1,n} & x_{2,n} \end{vmatrix}\neq 0. \tag{4}$$

如果不满足，可以对矩阵 $X=(\boldsymbol{x}_1,\boldsymbol{x}_2)$ 实施初等行变换使得 $X'=(\boldsymbol{x}'_1,\boldsymbol{x}'_2)=CX$ 满足上式，其中 C 为整数幺模 (行列式的绝对值为 1) 矩阵. 此时，若 $\boldsymbol{m}$ 为 $\boldsymbol{x}'_1$ 和 $\boldsymbol{x}'_2$ 的同步整数关系，则 $C^{\mathrm{T}}\boldsymbol{m}$ 为 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 的同步整数关系. 特别地，若 $\alpha=a+bI$ $(I=\sqrt{-1})$ 为 $b\neq 0$ 的代数数，则对 $j=0,1,2,\cdots$, 有

$$\begin{vmatrix} \mathrm{Re}(\alpha^j) & \mathrm{Im}(\alpha^j) \\ \mathrm{Re}(\alpha^{j+1}) & \mathrm{Im}(\alpha^{j+1}) \end{vmatrix}=b(a^2+b^2)^j\neq 0,$$

从而 $(1,\mathrm{Re}(\alpha),\cdots,\mathrm{Re}(\alpha^j))^{\mathrm{T}}$ 和 $(0,\mathrm{Im}(\alpha),\cdots,\mathrm{Im}(\alpha^j))^{\mathrm{T}}$ 满足上述假设.

定义 2　设 $\boldsymbol{x}_i=(x_{i,1},x_{i,2},\cdots,x_{i,n})^{\mathrm{T}}\in\mathbb{R}^n, i=1,2$. 将矩阵 $H\in\mathbb{R}^{n\times(n-2)}$ 称作是 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 的超平面矩阵, 如果 H 的各列形成向量空间 $X^{\perp}=\{\boldsymbol{y}\in\mathbb{R}^n:\boldsymbol{x}_i^{\mathrm{T}}\boldsymbol{y}=0, i=1,2\}$ 的一组基.

设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 为 $\mathbb{R}^n$ 的标准基，即 $\boldsymbol{b}_i$ 的第 i 个分量为 1, 其它分量为 0. 依次对 $\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_{n-2}$ 实施标准 Gram-Schmidt 正交化过程后得到 $\boldsymbol{x}_1^*,\boldsymbol{x}_2^*,\boldsymbol{b}_1^*,\boldsymbol{b}_2^*,\cdots,\boldsymbol{b}_{n-2}^*$. 由 $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ 满足 (4) 易知 $n\times(n-2)$ 矩阵 $(\boldsymbol{b}_1^*,\boldsymbol{b}_2^*,\cdots,\boldsymbol{b}_{n-2}^*)$ 就是 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 的一个超平面矩阵，记为 H_X.

定理 2 若对任意 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 的同步整数关系 $\boldsymbol{m}$ 和任意整数幺模矩阵 A, 均存在一个正交阵 $Q \in \mathbb{R}^{(n-2)\times(n-2)}$ 使得 $H = AH_XQ$ 是一个下梯形矩阵, 且每个对角元 $h_{j,j} \neq 0$, 则

$$\frac{1}{\max\limits_{1\leq j\leq n-2}|h_{j,j}|} \leq \|\boldsymbol{m}\|_2, \tag{5}$$

其中 $\|\boldsymbol{m}\|_2 = \sqrt{\langle \boldsymbol{m}, \boldsymbol{m}\rangle}$ 为 $\boldsymbol{m}$ 的 2- 范数.

定理 2 的证明思路与 [10] 中定理 1 类似, 在此不再赘述. 但应当指出的是上述定理提供了一条探测同步整数关系的途径: 若能够以左乘整数幺模矩阵, 右乘实正交矩阵的形式对超平面矩阵对角元的模进行约化, 则不等式 (5) 给出了任意 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 的同步整数关系 2- 范数的一个不断增加的下界. 而另一方面, 如果 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 存在同步整数关系, 那么这个下界便不会无限制的增加.

定义 3 设 $H = (h_{i,j}) \in \mathbb{R}^{n\times(n-2)}$ 满足 $h_{j,j} \neq 0$ 且对 $j > i$, 有 $h_{i,j} = 0$. 初始化 $D = (d_{i,j})$ 为 n 阶单位阵 I_n. 对 i 从 2 到 n , j 从 $\min\{i-1, n-2\}$ 到 1 (步长为 -1), 令 $q := \lfloor h_{i,j}/h_{j,j} \rceil$ (距 $h_{i,j}/h_{j,j}$ 最近的整数); 对 k 从 1 到 n, 令 $d_{i,k} := d_{i,k} - qd_{j,k}$. 此时, 更新 $H := DH$. 若 $h_{n-1,n-2} = 0$ 且 $h_{n,n-2} \neq 0$, 则交换 D 和 H 的最后两行. 称 H 为原矩阵的广义 Hermite 约化, D 为原矩阵的广义 Hermite 约化矩阵.

显然, 定义 3 中的矩阵 D 为一个整数幺模矩阵, 于是广义 Hermite 约化便是一种约化超平面矩阵的恰当方式, 依此可以得到一个探测同步整数关系的迭代算法 SIRD.

算法 1 (SIRD) 输入: $X = (\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathbb{R}^{n\times 2}$ 满足 (4), 参数 $\gamma > \frac{2}{\sqrt{3}}$ 和 $M > 0$. 或者输出 $\boldsymbol{x}_1, \boldsymbol{x}_2$ 的一个同步整数关系, 或者断言 X 不存在 2- 范数小于 M 的同步整数关系.

S1: 计算超平面矩阵 H_X. 初始化 $H := H_X$, $B = I_n$.

S2: 计算 H 的广义 Hermite 约化矩阵 D. 令 $X^{\mathrm{T}} := X^{\mathrm{T}}D^{-1}$, $H := DH$, $B := BD^{-1}$.

S3: 迭代.

S31: 选择 r 使得 $\gamma^r|h_{r,r}| \geq \gamma^i|h_{i,i}|$ $(1 \leq i \leq n-2)$. 交换 H 的第 r 行和第 $r+1$ 行, 交换 X^{T} 和 B 的第 r 列和第 $r+1$ 列.

S32: 若上一步选择的 $r < n-2$, 则 H 便不再是下梯形的, 此时对 H 作 LQ 分解 (等价于对 H^{T} 作 QR 分解), 更新 H 为分解后的下梯形矩阵.

S33: 计算 H 的广义 Hermite 约化矩阵 D. 令 $X^{\mathrm{T}} := X^{\mathrm{T}}D^{-1}$, $H := DH$, $B := BD^{-1}$.

S34: 计算 $G := \frac{1}{\max\limits_{1\leq j\leq n-2}|h_{j,j}|}$. 若 $G > M$, 则断言 X 不存在 2- 范数小于 M 的同步整数关系.

S35: 若 X^{T} 的第 j 列为 $\mathbf{0}$, 则输出 B 的第 j 列; 若 $h_{n-2,n-2} = 0$, 则输出 B 的第 $n-2$ 列.

定理 3 若 $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbb{R}^n$ 存在同步整数关系, 则 SIRD 算法一定能找出一个同步整数关系 $\boldsymbol{m}$, 且

$$\|\boldsymbol{m}\|_2 \leq \gamma^{n-2}\lambda(X), \tag{6}$$

其中 $\lambda(X)$ 为 $\boldsymbol{x}_1, \boldsymbol{x}_2$ 的同步整数关系具有的最小 2- 范数, $\gamma > \frac{2}{\sqrt{3}}$.

注 1 若 $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbb{R}^n$ 存在同步整数关系, 则在算法 1 中令 $M \geq \gamma^{n-2}\lambda(X)$ 即可. 该算法保证了输出同步整数关系的 2- 范数总小于或等于 M.

定理 3 前一部分的证明可参考文献 [11], 此处只简述式 (6) 为何成立. 设 $\boldsymbol{m}$ 是经过 $k+1$ 次迭代输出的同步整数关系. 可以证明 $\|\boldsymbol{m}\|_2 = \frac{1}{h_{n-2,n-2}(k)}$; 按照 S31 中 r 的选取又知: 当 $r=n-2$ 时, $\max|h_{j,j}(k)| \le \gamma^{n-2}|h_{n-2,n-2}(k)|$. 从而由定理 2 得

$$\lambda(X) \ge \frac{1}{\max|h_{j,j}(k)|} \ge \frac{\gamma^{2-n}}{|h_{n-2,n-2}(k)|} = \gamma^{2-n}\|\boldsymbol{m}\|_2.$$

SIRD 算法构造的超平面矩阵为一个实矩阵, 算法中的矩阵 B 和 D 的元素均不会有虚数出现, 从而克服了 PSLQ 对复数向量仅能输出 Gauss 整数关系的不足. 至此, 复数向量 $\boldsymbol{v} = (v_1, v_2, \cdots, v_2)^{\mathrm{T}}$ 的整数关系便可以由 SIRD 算法探测 $\boldsymbol{v}$ 的实部向量 $(\mathrm{Re}(v_1), \mathrm{Re}(v_2), \cdots, \mathrm{Re}(v_2))^{\mathrm{T}}$ 和虚部向量 $(\mathrm{Im}(v_1), \mathrm{Im}(v_2), \cdots, \mathrm{Im}(v_2))^{\mathrm{T}}$ 的同步整数关系得到.

例 1 设 $\alpha = 2 + \sqrt{3}I$. 欲求 α 在 $\mathbb{Z}[x]$ 中的极小多项式 $x^2 - 4x + 7$. 取 α 的四位有效数字的近似值 $\overline{\alpha} = 2.000 + 1.732I$. 于是得到 $\boldsymbol{v}_1 = (1, 2, 1)^{\mathrm{T}}$, $\boldsymbol{v}_2 = (0, 1.732, 6.928)^{\mathrm{T}}$. 对 $\boldsymbol{v}_1, \boldsymbol{v}_2$ 运行 SIRD 算法, 仅需要两次迭代就可以得到一组 $\boldsymbol{v}_1, \boldsymbol{v}_2$ 的同步整数关系. 迭代过程中的矩阵 B 如下

$$\begin{pmatrix} 2 & 1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 7 & 0 & 2 \\ -4 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix},$$

显然后一个矩阵的第一列即为所求. 若只取三位有效数字, 则 SIRD 算法通过 3 次迭代后输出 $(1213, -693, 173)^{\mathrm{T}}$, 这组输出尽管是 $(1, 2, 1)^{\mathrm{T}}$ 和 $(0, 1.73, 6.93)^{\mathrm{T}}$ 的同步整数关系, 但不再是 $(1, \alpha, \alpha^2)^{\mathrm{T}}$ 的整数关系. 因此为了近似重构代数数的极小多项式, 必须对误差进行控制.

3　误差控制

本文近似重构 n 次代数数极小多项式的基本思想是: 探测 $(1, \overline{\alpha}, \cdots, \overline{\alpha}^n)^{\mathrm{T}}$ 的一组整数关系 $(p_0, p_1, \cdots, p_n)^{\mathrm{T}} \in \mathbb{Z}^{n+1}$ (当 α 为实代数数时用 PSLQ 算法 [10]; 当 α 为虚代数数时用上一节介绍的 SIRD 算法), 使得 $p(x) = \sum_{i=0}^{n} p_i x^i$ 满足 $|p(\overline{\alpha})| = 0$. 利用定理 1 便可以保证该多项式就是 α 的极小多项式. 为证定理 1, 需做如下准备.

引理 1 设 f 是一个 n 次单变元多项式. 若 $\max\limits_{1\le i\le n}|\alpha^i - \overline{\alpha}^i| \le \varepsilon$, 则 $|f(\alpha) - f(\overline{\alpha})| \le \varepsilon \cdot n \cdot \mathrm{height}(f)$.

证　设 $f = \sum_{i=0}^{n} f_i x^i$. 则

$$|f(\alpha) - f(\overline{\alpha})| = \left|\sum_{i=1}^{n} f_i(\alpha^i - \overline{\alpha}^i)\right| \le \varepsilon \cdot n \cdot \mathrm{height}(f).$$

定义 4 设 m 次多项式 $g = \sum_{i=0}^{m} g_i x^i \in \mathbb{Z}[x]$ 的所有复根为 $z_1, z_2, \cdots, z_m$. 定义 g 的 Mahler 度量为

$$M(g) = |g_m| \prod_{j=1}^{m} \max\{1, |z_j|\}.$$

代数数 α 的 Mahler 度量定义为其极小多项式的 Mahler 度量，记为 $M(\alpha)$.

引理 2[13] 设 $\alpha_1,\alpha_2,\cdots,\alpha_q$ 为次数分别为 $d_1,d_2,\cdots,d_q$ 的代数数. 令 $D=[\mathbb{Q}(\alpha_1,\alpha_2,\cdots,\alpha_q):\mathbb{Q}]$. 设 $P\in\mathbb{Z}[x_1,x_2,\cdots,x_q]$ 关于 x_h 的次数不超过 N_h $(1\le h\le q)$. 若 $P(\alpha_1,\alpha_2,\cdots,\alpha_q)\neq 0$, 则

$$|P(\alpha_1,\alpha_2,\ldots,\alpha_q)|\ge\|P\|_1^{1-D}\prod_{h=1}^{q}M(\alpha_h)^{\frac{-DN_h}{d_h}},$$

其中 $\|P\|_1$ 表示 P 的 1- 范数, 即所有系数绝对值之和.

对任意的多元多项式 $P\in\mathbb{Z}[x_1,x_2,\cdots,x_q]$, 若 $P(\alpha_1,\alpha_2,\cdots,\alpha_q)\neq 0$, 则上述引理给出了一个关于 $|P(\alpha_1,\alpha_2,\cdots,\alpha_q)|$ 的下界. 若将其应用到 $\mathbb{Z}[x]$ 中的多项式，则得到

推论 1 设 α 为一个 n_0 次的代数数， $g(x)=\sum\limits_{i=0}^{m}g_ix^i\in\mathbb{Z}[x]$, 且 α 和 $g(x)$ 的高度均不超过 H. 若 $g(\alpha)\neq 0$, 则 $|g(\alpha)|\ge(m+1)^{-(n_0-1)}\cdot(n_0+1)^{-\frac{m}{2}}\cdot H^{-(m+n_0-1)}$.

证 由引理 2 得

$$\begin{aligned}|g(\alpha)|&\ge\|g\|_1^{1-n_0}M(\alpha)^{-m}\\&\ge((m+1)\mathrm{height}(g))^{1-n_0}M(\alpha)^{-m}\\&\ge((m+1)\mathrm{height}(g))^{1-n_0}((n_0+1)^{\frac12}\mathrm{height}(\alpha))^{-m},\end{aligned}\tag{7}$$

再由 α 和 $g(x)$ 的高度均不超过 H, 结论得证. 其中 (7) 中的第 2 个不等号是因为 $\mathrm{height}(g)\le\|g\|_1\le(m+1)\mathrm{height}(g)$, 第 3 个不等号是由 Landau 不等式 [14] $M(\alpha)\le\|p\|_2$ 及 $\mathrm{height}(p)\le\|p\|_2\le\sqrt{n+1}\mathrm{height}(p)$ 得到的，其中 $p=\sum\limits_{i=0}^{n_0}p_ix^i\in\mathbb{Z}[x]$ 为 α 的极小多项式， $\|p\|_2$ 表示其 2- 范数，即 $\|p\|_2=\Big(\sum\limits_{i=0}^{n_0}p_i^2\Big)^{\frac12}$. 证毕.

定理 1 的证明 必要性由 $|p(\overline{\alpha})|=|p(\overline{\alpha})-p(\alpha)|\le\varepsilon\cdot n\cdot H$ 易得；由 $|p(\alpha)|-|p(\overline{\alpha})|\le|p(\alpha)-p(\overline{\alpha})|$ 知 $|p(\alpha)|\le|p(\overline{\alpha})|+\varepsilon\cdot n\cdot H<(n+1)^{1-\frac32 n}H^{1-2n}$, 从而由推论 1 得 $p(\alpha)=0$, 充分性得证. 证毕.

定理 1 保证了能够通过近似值 $\overline{\alpha}$ 得到其对应准确值的极小多项式. 结合 (2) 和 (6), 并令 $\gamma=2$ 便得到基于整数关系探测算法近似重构代数数极小多项式的误差控制条件.

推论 2 设 α 和 $\overline{\alpha}$ 意义同上，且满足

$$\max_{1\le i\le n}|\alpha^i-\overline{\alpha}^i|<\max\{2^{-2n^2+4n}(n+1)^{-\frac52 n},\,2^{-n^2+2n}(n+1)^{-2n}\}\cdot H^{-2n}.\tag{8}$$

则对 $i=1,2,\cdots,n$, 一个 $\overline{\boldsymbol{v}}=(1,\overline{\alpha},\cdots,\overline{\alpha}^i)^{\mathrm{T}}$ 的高度不超过 $2^{n-2}\sqrt{n+1}H$ 的整数关系一定同时是 $\boldsymbol{v}=(1,\alpha,\cdots,\alpha^i)^{\mathrm{T}}$ 的整数关系.

证 取最大值的两个部分是分别将 (2) 中的 H, 定理 1 中的 $p(x)$ 和推论 1 中 $g(x)$ 的高度的上界 H 替换为 $2^{n-2}\sqrt{n+1}H$ 得到的. 证毕.

推论 2 并未保证 $\boldsymbol{v}$ 的一个高度不超过 $2^{n-2}\sqrt{n+1}H$ 的整数关系一定同时是 $\overline{\boldsymbol{v}}$ 的整数关系. 即通过上述误差控制，利用算法 1 并不能保证得到 $\overline{\boldsymbol{v}}$ 的高度不超过 $2^{n-2}\sqrt{n+1}H$ 同步

整数关系. 但是由定理 1, 对某一个 $i \in \{1,2,\cdots,n\}$ 一定存在高度不超过 $2^{n-2}\sqrt{n+1}H$ 的一组向量 $\boldsymbol{p}$, 使得

$$|\langle \overline{\boldsymbol{v}}, \boldsymbol{p}\rangle| < \delta, \tag{9}$$

其中 $\delta = 2^{-2n^2+5n-3}(n+1)^{-\frac{5}{2}n+\frac{3}{2}}H^{-2n+1}$. 比如, α 极小多项式的系数向量便满足上式. 为了找出这样的整数向量, 需要对算法 1 的 S35 作如下调整, 得到算法 1′:

S35′: 记 X^{T} 的第 i 列为 $\begin{pmatrix} x_{i1} \\ x_{i2} \end{pmatrix}$. 若 $|x_{j1}|$ 和 $|x_{j2}|$ 同时小于 $\frac{\delta}{\sqrt{2}}$, 则输出 B 的第 j 列; 若 $h_{n-2,n-2} = 0$, 则输出 B 的第 $n-2$ 列.

基于上述分析, 在 (8) 的误差控制下, 对实代数数用改进的 PSLQ 算法 [9], 虚代数数用算法 1′ 便得到一个解决问题 1 的完备算法.

算法 2 输入: 未知代数数 α 的满足 (8) 的近似值 $\overline{\alpha}$, α 次数的上界 n 和高度的上界 H. 输出: α 的极小多项式.

E1: 对 i 从 1 到 n 循环

E11: 构造向量 $\boldsymbol{v} := (1, \overline{\alpha}, \cdots, \overline{\alpha}^i)^{\mathrm{T}}$.

E12: 令 $M = 2^{n-2}\sqrt{n+1}H$. 以 $\boldsymbol{v}$, M 为输入调用整数关系探测算法 PSLQ 或算法 1′.

E121: 若整数关系探测算法输出向量 $(p_0, p_1, \cdots, p_i)^{\mathrm{T}}$, 则输出多项式 $\sum_{k=0}^{i} p_k x^k$ 的本原部分.

定理 4 设一未知代数数 α 的次数不超过 n, 高度不超过 H. 若 α 的近似值 $\overline{\alpha}$ 满足 (8), 则算法 2 将正确输出 α 准确的极小多项式.

证　设 α 的精确次数为 $n_0 (\leq n)$. 当算法 2 中的 $i < n_0$ 时, 不可能有输出. 假设此时有输出. 这意味着整数关系探测算法返回了一个高度不超过 $M = 2^{n-2}\sqrt{n+1}H$ 的的整数向量, 并且满足 (9). 而由这两点, 结合误差控制条件 (8) 便可以得到该输出就是准确的极小多项式, 与 $i < n_0$ 矛盾. 当 $i = n_0$ 时, 算法 2 一定能返回正确的极小多项式. 这是因为定理 3 作相应调整后对算法 1′ 仍然成立: 若满足 (9) 的 $\boldsymbol{p}$ 存在, 则算法 1′ 一定能找到. 所以对 $\overline{\boldsymbol{v}} = (1, \overline{\alpha}, \cdots, \overline{\alpha}^{n_0})^{\mathrm{T}}$, 算法 1′ 一定会输出一个整数向量. 若 $h_{n-2,n-2} = 0$, 则输出是 $\overline{\boldsymbol{v}}$ 的整数关系; 否则输出的整数向量满足 (9). 尽管这个整数向量可能不是 $\overline{\boldsymbol{v}}$ 的整数关系, 但在 (8) 的误差控制下定理 1 保证了它必定是 $(1, \alpha, \cdots, \alpha^{n_0})^{\mathrm{T}}$ 的整数关系. 所以, 从该整数向量必能得到 α 准确的极小多项式. 证毕.

4　数值结果

值得注意的是上述正确性和终止性都是在精确的实数计算模型意义下得到的. 在计算机实现时, 由于涉及实数操作, PSLQ 算法, SIRD 算法以及本文的算法 2 不能得到精确实施, 但可以使用高精度的程序包, 如 ARPREC[15], GNU 高精度算法库 [16] 等. 通用的商业计算机代数系统 Maple 和 Mathematica 都支持高精度的运算. 本文作者在计算机代数系统 Maple 13 中实现了 SIRD 算法和算法 2, 开发了 sird 程序包.

算法 2 的实现中, 涉及到实代数数的处理时, 直接调用 Maple 13 自带的 PSLQ 命令; 由于采用高精度运算, 只能保证对 $\boldsymbol{v} = (1, \overline{\alpha}, \cdots, \overline{\alpha}^i)^{\mathrm{T}}$ 探测近似的 (同步) 整数关系, 即可以求出

一组整数向量 $\boldsymbol{p}=(p_0,p_1,p_2,\cdots,p_i)^{\mathrm{T}}$, 使得 $\langle \boldsymbol{v},\boldsymbol{p}\rangle$ 充分接近于 0. 为了进一步保证程序输出的正确性, 在得到整数关系 $\boldsymbol{p}_i$ 后, 程序中还利用式 (3) 中对应的条件 (H 替换为 $2^{n-2}\sqrt{n+1}H$) 作为判断其是否确为 $\bar{\alpha}$ 所对应的准确极小多项式系数的依据.

本节所有的数值实验都是使用 2GB 内存, AMD Athlon™ 7750 处理器 (2.70 GHz) 的机器在 Windows XP 下用 Maple 13 计算出来的. [1]

例 2[3] 设 α 为一未知的正有理数, 即次数为 1 的代数数, 其分母绝对值的上界为 $H=170$. 此例中分母的上界恰好是该有理数高度的上界. 首先 (8) 给出的误差控制为 $\varepsilon\le\frac{1}{\sqrt{2}H^2}=\frac{\sqrt{2}}{57800}$. 在此误差控制下通过某种数值方法得到该有理数的一个近似值 $\bar{\alpha}=0.8106335868$, 在计算过程中将精度设置为 $-\lfloor\log_{10}(\frac{\sqrt{2}}{57800})\rfloor=5$ 位, 执行下面的命令

[> read sird; Digits := -floor (evalf (log[10] (sqrt(2)/57800)));

[> f := ExactMinimalPolynomial (0.8106335868, 1, 170);

输出 $f:=-137+169*\_X$, 即 α 的极小多项式, 其中命令 ExactMinimalPolynomial 是 sird 包中对算法 2 的实现. 由此得出 α 的准确值为 $\frac{137}{169}$. 运行

[> f := ExactMinimalPolynomial(0.81063, 1, 170);

同样输出 $f:=-137+169*\_X$, 而运用 [3] 中的算法对近似值 $\bar{\alpha}=0.81063$ 仅仅能够返回 $\frac{107}{132}$. 这再次说明了本文误差控制条件的优势.

注 2 当 α 是有理数时, [3] 中的算法只需知道分母绝对值的上界, 而本文中的算法需要知道该有理数高度的上界, 即分子分母绝对值的最大值的上界. 在实际应用时, 若只知道分母绝对值的上界, 则将得到的近似值分成整数部分和小数部分, 然后对小数部分应用算法 2 将其恢复成准确值即可. 由于整数部分本身就是精确的, 因此结果仍是精确的.

注 3 此例中若将 Digits 设成一个小于 5 的正整数, 则不能返回准确结果. 这说明 (8) 的误差控制在转化成精确十进制表示时是比较精确的. 另外, 若将 Digits 设成一个大于 5 的整数, 则对应的近似值也需提高到相应精度才能保证结果的准确性.

在引言部分已经提到, 利用 LLL 算法也可以解决问题 1. 计算机代数系统 Maple 13 已经集成了该功能, 即 PolynomialTools 包中的 MinimalPolynomial 命令. 但是其实现方法并不能保证得到该代数数的极小多项式, 而仅仅能够得到一个以该近似代数数为根的整系数多项式. 为了将本文算法和基于 LLL 的算法进行比较, sird 程序包中也包含了一个基于 SIRD 的与 MinimalPolynomial 命令具有相同功能的命令 MiniPoly.

例 3 设 $\alpha=\sqrt[5]{23}+\sqrt[6]{7}$. 易知其次数为 30. 若想求得 α 的极小多项式, 可以采用算法 2 通过其近似值重构获得. 经试验, 当 Digits:=300 时, 算法 2 便能保证输出正确结果. 通过某种近似计算方法得到一个 α 的具有 300 位准确十进制表示的近似值 $a=3.2552587848233\cdots$, 并运行如下命令

[> Digits := 300: p_SIRD := MiniPoly(a, 30);

经过 9.718 秒的运算, 最终输出的多项式 p_SIRD 是一个 30 次的不可约多项式, 经验证确为 α 的极小多项式. 而运行 Maple 13 中自带的命令

[> PolynomialTools:-MinimalPolynomial(a, 30);

1. 程序和例子可以通过访问 http://cid-5dbb16a211c63a9b.office.live.com/self.aspx/.Public/MiniPoly.rar 得到.

经过 9.218 秒的运算，输出一个错误的多项式. 这并不是 Maple 13 的失误，而是由其算法本身需要的高精度导致的. 若将 Digits 设为 398, 则 Maple 13 自带的命令经 13.719 秒获得正确的结果.

经多次试验发现，当 Digits 不大时， MiniPoly 的运行时间略长于 MinimalPolynomial. 但当 Digits 较大时，如例 3 所示，算法 2 运行时间更优. 因此算法 2 对较大规模问题有较好的效果. 例如利用 MiniPoly 命令可以成功地从代数数 $3^{1/6}-I*2^{1/7}$ 的近似值重构出其准确的极小多项式，其次数为 84, 高度为 3029254676588448.

算法 2 可以应用到有理数域上的一元多项式因式分解. 其基本思想是先求出待分解多项式的一个适当精度的近似根，然后利用算法 2 可以得到该根准确的极小多项式，而该极小多项式就是原多项式的一个因子. 对原多项式除以该因子后得到的多项式重复以上过程，直到得到原多项式完全的不可约分解. 尽管该方法并不新颖，效率也不比现有的分解算法高，但该方法的中间步骤都采用近似计算，输出结果却是精确的. 因此，仍不失为一个符号和数值混合计算 [17] 的成功案例.

例 4 采用上述策略分解一元整系数多项式

$$g=3650+6745\_X^6-1188\_X^5-5973\_X^3+10094\_X^2-7916\_X \\ +4601\_X^4+4200\_X^{10}+560\_X^9-6263\_X^7+4650\_X^8.$$

该多项式无实根，因此 [9] 中的分解方法不再奏效. 首先运行如下命令

[> Digits := 51: a := fsolve(g, _X, complex)[1];

得到 g 的一个复近似根，然后调用 sird 包中的 ExactMinimalPolynomial 命令

[> f1 := ExactMinimalPolynomial (a, 10, 256*90106990^ (1/2));

便得到该近似根对应的准确极小多项式 $50-42\_X+40\_X^2+7\_X^3+10\_X^5+75\_X^6$, 它自然是 g 的一个不可约因子，其中 $256\sqrt{90106990}$ 为该近似根对应的准确代数数高度的上界，是利用 Mignotte 界 [14] 得到的. 再通过多项式除法得到 $\frac{g}{f1}=56\_X^4+62\_X^2-97\_X+73\equiv \_X^4+2\_X^2+3\_X+3 \bmod 5$ 不可约，从而完成在有理数域上对 g 的因式分解.

5　结论和展望

对任意的复代数数，本文在其近似值和准确的极小多项式之间建立了一座桥梁. 在已知某代数数次数和高度上界的情形下，只要预先得到该代数数的一个满足 (8) 的近似值，算法 2 便能有效地给出该近似代数数的准确值的极小多项式. 这便有力地推动了 “采用近似计算获得准确值” 这一问题的研究，使其适用范围扩大到任意的代数数. 并且本文的算法可以应用于因式分解等诸多实际问题中去.

然而，由于本文算法的实施采用了高精度的浮点运算，尽管有大量的实验数据说明本文算法在数值方面表现良好，但是对算法的数值特性和位复杂度还缺少理论层面的分析.

参　考　文　献

[1] Kannan R, Lenstra A K, and Lovász L. Polynomial factorization and nonrandomness of bits of

algebraic and some transcendental numbers. *Math. Comput.*, 1988, **50**(181): 235–250.
[2] Wang X and Pan V Y. Acceleration of euclidean algorithm and rational number reconstruction. *SIAM J. Comput.*, 2003, **32**: 548–556.
[3] Zhang J Z and Feng Y. Obtaining exact value by approximate computations. *Science in China Series A: Mathematics*, 2007, **50**(9): 1361–1368.
[4] Lenstra A K, Lenstra H W, and Lovász L. Factoring polynomials with rational coefficients. *Math. Ann*, 1982, **261**: 515–534.
[5] Schönhage A. Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. *LNCS*, 1984, **172**: 436–447.
[6] Nguên P Q and Stehlé D. Floating-point LLL revisited. *LNCS*, 2005, **3494**: 215–233.
[7] Morel I, Stehlé D, and Villard G. H-LLL: Using Householder inside LLL, In ISSAC '09, 2009: 271–278.
[8] Mark van Hoeij and Andrew Novocin, Gradual sub-lattice reduction and a new complexity for factoring polynomials. *LNCS*, 2010, **6034**: 539–553.
[9] Qin X L, Feng Y, Chen J W, et al. Finding exact minimal polynomial by approximations. SNC '09, 2009: 125–131.
[10] Ferguson H R P, Bailey D H, and Arno S. Analysis of PSLQ, an integer relation finding algorithm. *Math. Comput.*, 1999, **68**(225): 351–369.
[11] Chen J W, Feng Y, Qin X L, et al. Detecting simultaneous integer relations for real vectors. 2010, http://arxiv.org/abs/1010.1982.
[12] Ferguson H R P and Forcade R W. Generalization of the euclidean algorithm for real numbers to all dimensions higher than two. *Bull. Amer. Math. Soc.*, 1979, **1**(6): 912–914.
[13] Mignotte M and Waldschmidt M. Linear forms in two logarithms and Schneider's method. *Math. Ann.*, 1978, **231**: 241–267.
[14] Gathen J V Z and Gerhard J. Modern Computer Algebra. London: Cambridge University Press, 1999.
[15] Bailey D H. A Fortran-90 Based Multiprecision System. *ACM Transactions on Mathematical Software*, 1995, **21**(4): 379–387.
[16] The GNU Multiple Precision Arithmetic Library. http://gmplib.org/.
[17] 支丽红. 符号和数值混合计算. 系统科学与数学, 2008, **28**(8): 1040–1052.

RECONSTRUCTING MINIMAL POLYNOMIAL FROM APPROXIMATE ALGEBRAIC NUMBERS

CHEN Jingwei, FENG Yong, QIN Xiaolin ZHANG Jingzhong

(*Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences, Chongqing* 401122; *Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu* 610041; *Graduate University, Chinese Academy of Sciences, Beijing* 100049)

Abstract This paper gives an error condition for reconstructing the minimal polynomial of an algebraic number from its approximation, and then present a newly complete algorithm to obtain the exact minimal polynomial from an approximate value by simultaneous integer relations detection. This work extends the applicable area of "obtaining exact value by approximate computations" from the rational to algebraic numbers.

Key words Simultaneous integer relation, algebraic number, minimal polynomial.