文章编号:1009-3087(2010)02-0126-06

采用近似方法的实代数数准确表示及其应用

秦小林[1,2,3],冯 勇[1*],陈经纬[2,3],李 骏[2,3]
(1. 电子科技大学 计算机推理与可信计算实验室,四川 成都 610054;2. 中国科学院 成都计算机应用研究所,四川 成都 610041;
3. 中国科学院 研究生院,北京 100049)

摘 要:针对如何保证实代数数的二进制展开不形成伪随机序列的问题,提出了通过实代数数的近似值重构它的准确极小多项式的算法,以此为基础提供了一种新的计算机实代数数表示方法。采用1个三元组序列:适当误差控制的实代数数近似值,极小多项式的次数和高度的上界。与目前的3种实代数数的计算机表示方法相比,在稀疏极小多项式情况下,新表示方法占有的二进制比特位与区间方法一致,低于符号方法,而略高于序方法;在稠密极小多项式情况下,比目前的3种表示方法都低。同时利用近似值重构极小多项式的方法,可获得多项式的准确因式分解。通过理论的分析和试验的验证,显示新的实代数数准确表示方法和应用是高效合理的。

关键词:实代数数;近似计算;符号计算;符号与数值混合计算
中图分类号:TP301 **文献标识码**:A

Exact Representation of Real Algebraic Number by Approximations and Its Applications

QIN Xiao-lin[1,2,3], *FENG Yong*[1*], *CHEN Jing-wei*[2,3], *LI Jun*[2,3]
(1. Lab. of Computer Reasoning and Trust. Comput., UESTC, Chengdu 610054, China;
2. Chengdu Inst. of Computer Applications, CAS, Chengdu 610041, China; 3. Graduate School of the Chinese Academy of Sciences, Beijing 100049, China)

Abstract: In order to make sure that the binary expansions of real algebraic numbers do not form secure pseudorandom sequences, a new algorithm was proposed to obtain the exact minimal polynomial from an approximate real algebraic number. Based on the algorithm, a new computer representation of real algebraic number was provided by using an ordered triple as an approximate real algebraic number within error controlling, the degree and the upper bound of height of its minimal polynomial. Compared with the popular three representations of real algebraic number, the binary bit operations of the new representation was consistent with that of the interval method, less than that of the sign representation, somewhat more than that of the order representation for the sparse minimal polynomial. However, the bits of the present representation was less than that of the three representations for the dense minimal polynomial. The proposed method can be used to obtain the exact factors of the polynomial via reconstruction of minimal polynomial from the approximate real algebraic number.

Key words: real algebraic number; approximate computation; symbolic computation; symbolic-numerical computation

收稿日期:2009-02-13
基金项目:国家973计划资助项目(2004CB318003);中国科学院知识创新重要方向项目(KJCX2-YW-S02);国家自然科学基金资助项目(10771205)
作者简介:秦小林(1980-),男,博士生. 研究方向:自动推理;符号与数值混合计算;符号计算.
*通讯联系人. E-mail: yongfeng@casit.ac.cn

数值计算具有速度快、能运用浮点运算处理近似问题,得到近似解和解决大规模问题的优势,已广泛应用于工程技术等领域。但它的主要问题是计算的不稳定性,同时一般只能得到局部解和部分解,因而遗漏某些有意义的解。相反,符号计算的主要特点是计算结果准确和计算过程稳定,已广泛应用于需要获得准确结果的领域,诸如计算机自动推理、可验证计算等。但它的劣势是计算复杂度高,在实际应用中效率不高,只能解决中小规模问题。因此,研究符号与数值混合计算就应运而生,混合计算即是把符号计算与数值计算结合起来:运用符号计算来处理近似奇异或对扰动敏感的病态问题,而用数值方法来加速符号计算的某一部分或计算可靠的近似解,尤其是应用数值计算方法来解决符号计算方法中的中间过程膨胀问题。近二十多年来,众多国内外学者将数值近似计算应用到符号计算领域,研究多项式的近似因式分解、多项式的近似最大公因式以及计算函数分解、检测一个多项式的不可约性和计算多项式的零点等问题,然而这些结果与准确计算结果还有一定的误差,都是近似的。近似方法与准确结果之间有一条天然的鸿沟[1]。

最近,采用近似计算获得准确结果领域取得重要突破,将高效的数值计算方法应用于符号计算问题中。张景中院士等提出的采用近似计算获取准确值的算法解决了浮点数到有理数的重构问题,为混合计算获取准确值这条鸿沟架起了一座桥梁[2],并将该算法成功地应用于多元多项式因式分解[3]。然而,在他们的工作中未涉及关于高次代数数(包括二次实代数数)的重构问题,即给定某个代数数的近似值如何获得它对应的极小多项式与准确结果。在信息安全中,该工作最早由著名计算机科学家图灵奖获得者 Manuel Blum 提出如何在计算机中保证代数数的二进制展开不形成伪随机序列[4],随后由 R. Kannan, A. K. Lenstra 和 L. Lovász 采用 LLL (Lenstr-Lenstra-Lovasz lattice reduction algorithm)算法进行了解答[5],由于 LLL 算法的局限性,导致他们实现的算法数值计算不稳定。因此,作者采用了具有高效、稳定的带参数的整数关系算法[6],基于该算法提出了一种新的高效的实代数数的计算机表示方法。

目前关于实代数数的表示都仅局限于区间方法、符号方法和序方法源自于文献[7],第一种方法直观,但不能得到准确实代数数本身,后两种方法准确,但不直观,并且 3 种方法所表示的实代数数的元组都需要存储它的极小多项式本身;另一方面有一些关于连分数展开的表示形式,如文献[8-12],以及改进和推广了 S. Lang 和 H. Trotter 的关于代数数连分数展开的算法[13],如文献[14-15]。他们的工作都仅对局部类型的代数数的表示进行了讨论。作者提出的近似方法的实代数数准确表示针对所有的类型,并且表示仅依赖于它的近似值、对应极小多项式的次数和高度,即三元组序列 $\langle\alpha\rangle = \langle\tilde{\alpha}, n, N\rangle$,其中,$\alpha$ 为某个实代数数,$\tilde{\alpha}$ 为它的近似值,n 和 N 分别为它对应的极小多项式的次数与高度上界。在稀疏极小多项式情况下,作者提出的表示方法占有的二进制比特位与已有的区间方法一致,低于符号方法,略高于序方法;在稠密极小多项式情况下,比目前的 3 种表示方法都低。因此新的表示方法大量节省了存储空间,并为实代数数的比较、符号判定以及计算机表示开辟了一条新的途径,同时利用作者提出的通过近似值重构极小多项式获得了多项式的准确因子。

作者要解决的问题是:如何控制实代数数的近似值 $\tilde{\alpha}$ 的精度以及外加什么条件才能决定唯一的实代数数 α。

1　带参数的整数关系算法

在这一部分,首先给出了一些相关的记号,然后简单介绍了与本文有关的改进的带参数的整数关系算法。

1.1　相关记号

纵观全文,将用 $\mathbb{Z}$ 表示整数域,$\mathbb{Q}$ 为有理数域,$\mathbb{R}$ 为实数域,$\mathbb{C}$ 为复数域。事实上,所有讨论的结果都可以推广到 $\mathbb{C}$ 中。$\mathbb{R}^n$ 表示实 n 维向量空间,$O(\mathbb{R})^n$ 表示 $\mathbb{R}$ 中组成的 n 维系统,$GL(n, O(\mathbb{R}))$ 为 $\mathbb{R}$ 中的幺模矩阵群,$U(n-1,\mathbb{R})$ 为 $\mathbb{R}$ 中的幺矩阵群,$\mathbb{Z}[x]$ 为整系数多项式环。$\mathrm{col}_j \boldsymbol{B}$ 表示取矩阵 $\boldsymbol{B}$ 的第 j 列元素,$|\cdot|$ 表示数取绝对值,多项式、向量与矩阵取 Frobenius 范数,即 $\|A\| = \left(\sum a_{i,j}^2\right)^{\frac{1}{2}}$,$\|\cdot\|_1$ 表示取整系数多项式的一范数,对多项式 $f = \sum_{i=0}^{n} a_i x^i$,$\|f\|_1 = \sum_{i=0}^{n} |a_i|$,$\|\cdot\|_\infty$ 表示取整系数多项式的无穷范数,对多项式 $f = \sum_{i=0}^{n} a_i x^i$,$\|f\|_\infty = \max_{0\le i\le n} |a_i|$,即多项式的高。

1.2　整数关系算法

定义 1　有整数序列 $x_1, x_2, \cdots, x_n$,如果存在不

全为零的整数 $a_1,a_2,\cdots,a_n$，使得 $\sum_{i=1}^{n} a_i x_i = 0$，称 $a_1,a_2,\cdots,a_n$ 为 $x_1,x_2,\cdots,x_n$ 的整数关系。

对给定向量 $\boldsymbol{x} = [x_1,x_2,\cdots,x_n]^{\mathrm{T}}$，如果 $\boldsymbol{a}\cdot\boldsymbol{x} = 0$，其中，非零向量 $\boldsymbol{a} \in \mathbb{Z}^n$，称 $\boldsymbol{a}$ 为 $\boldsymbol{x}$ 的向量整数关系。

为方便介绍获得向量整数关系算法，下面给出一些重要的定义与定理，更多的细节请参考文献[6]。

定义2 设 $\boldsymbol{x} = [x_1,x_2,\cdots,x_n]^{\mathrm{T}} \in \mathbb{R}^n$，其 Frobenius 范数 $|\boldsymbol{x}|$ 为1。在 $\mathbb{R}^n$ 上定义 $\boldsymbol{x}^{\perp}$ 是所有与 $\boldsymbol{x}$ 正交的向量集，$O(\mathbb{R})^n \cap \boldsymbol{x}^{\perp}$ 是 $\boldsymbol{x}$ 的整数关系的离散格，$M_{\boldsymbol{x}} > 0$ 是对 $\boldsymbol{x}$ 的任何整数关系最小的 Frobenius 范数。

定义3 设 $\boldsymbol{x} = [x_1,x_2,\cdots,x_n]^{\mathrm{T}} \in \mathbb{R}^n$，其 Frobenius 范数 $|\boldsymbol{x}|$ 为1，其中，$\boldsymbol{x}$ 的元素都不为零，即：对 $1 \leqslant j \leqslant n$，$x_j \neq 0$（否则有明显的整数关系）。对 $1 \leqslant j \leqslant n$ 定义部分和为：$s_j^2 = \sum_{j \leqslant k \leqslant n} x_k^2$，考虑单位向量 $\boldsymbol{x}$，定义 $n \times (n-1)$ 下梯形矩阵 $\boldsymbol{H}_{\boldsymbol{x}} = (h_{i,j})$，其中，

$$h_{i,j} = \begin{cases} 0 & \text{如果 } 1 \leqslant i < j \leqslant n-1, \\ s_{i+1}/s_i & \text{如果 } 1 \leqslant i = j \leqslant n-1, \\ -x_i x_j/(s_j s_{j+1}) & \text{如果 } 1 \leqslant j < i \leqslant n。 \end{cases}$$

式中，$h_{i,j}$ 是标度不变的。

定义4 设 $\boldsymbol{H}$ 是下梯形矩阵，形如：对 $j > i$，有 $h_{i,j} = 0$ 且 $h_{j,j} \neq 0$。初始化 $\boldsymbol{D} = \boldsymbol{I}_n$，定义矩阵 $\boldsymbol{D} = (d_{i,j}) \in GL(n,O(\mathbb{R}))$，其中，$d_{i,j}$ 递归地定义如下：对 i 从2到 n，j 从 $i-1$ 到1（步长为 -1），令 $q = \mathrm{nint}(h_{i,j}/h_{j,j})$；对 k 从1到 j，将 $h_{i,k} - qh_{j,k}$ 赋予 $h_{i,k}$，同时 k 从1到 n，将 $d_{i,k} - qd_{j,k}$ 赋予 $d_{i,k}$，其中，函数nint是取最靠近分数的整数，即：$\mathrm{nint}(t) = \lfloor t + 1/2 \rfloor$，以上的约化过程称为改进的 Hermite 约化。

定理1[6] 设向量 $\boldsymbol{x} \neq 0 \in \mathbb{R}^n$，如果 $\boldsymbol{x}$ 的整数关系 $\boldsymbol{m}$，对任意矩阵 $\boldsymbol{A} \in GL(n,O(\mathbb{R}))$，存在单位阵 $\boldsymbol{Q} \in U(n-1)$，使得 $\boldsymbol{H} = \boldsymbol{A}\boldsymbol{H}_{\boldsymbol{x}}\boldsymbol{Q}$ 是下梯形矩阵且对角元满足 $h_{j,j} \neq 0$，那么

$$\frac{1}{\max\limits_{1 \leqslant j \leqslant n-1} |h_{j,j}|} = \min_{1 \leqslant j \leqslant n-1} \frac{1}{|h_{j,j}|} \leqslant |\boldsymbol{m}|。$$

定理2[6] 设 $n \geqslant 2$，$\tau > 1$，$\gamma > \sqrt{4/3}$，有向量 $\boldsymbol{x} \neq 0 \in \mathbb{R}^n$ 在 $O(\mathbb{R})^n$ 上的整数关系。如果 $M_{\boldsymbol{x}}$ 是对 $\boldsymbol{x}$ 的任何整数关系最小的 Frobenius 范数，那么带参数 τ 的整数关系算法找到对应整数关系的迭代次数不超过 $\binom{n}{2}\frac{\log(\gamma^{n-1}M_{\boldsymbol{x}})}{\log\tau}$。

定理3[6] 设 $M_{\boldsymbol{x}}$ 是对 $\boldsymbol{x}$ 的任何整数关系最小的 Frobenius 范数，整数关系 $\boldsymbol{m}$ 是带参数 τ 的算法得到，那么对任意实向量有

$$\gamma > \sqrt{4/3} \quad \text{且} \quad |\boldsymbol{m}| \leqslant \gamma^{n-2} M_{\boldsymbol{x}}。$$

基于上述定理，并假设存在误差控制 ε，得到如下的整数关系算法。

算法1 改进的带参数的整数关系算法

输入：向量 $\boldsymbol{x}$ 和误差控制 ε

输出：整数关系 $\boldsymbol{m}$

步骤1：令 $i := 1$，$\tau > 2/\sqrt{3}$，单位化向量 $\boldsymbol{x}$ 为 $\bar{\boldsymbol{x}}$；

步骤2：依据定义3构造 $\boldsymbol{H}_{\bar{\boldsymbol{x}}}$；

步骤3：用改进的 Hermite 约化生成矩阵 $\boldsymbol{D} \in GL(n,O(\mathbb{R}))$；

步骤4：设 $\bar{\boldsymbol{x}} := \bar{\boldsymbol{x}}\cdot\boldsymbol{D}^{-1}$，$\boldsymbol{H} := \boldsymbol{D}\cdot\boldsymbol{H}$，

$\boldsymbol{A} := \boldsymbol{D}\cdot\boldsymbol{A}$，$\boldsymbol{B} := \boldsymbol{B}\cdot\boldsymbol{D}^{-1}$，

情况1：如果 $\bar{x}_j = 0$，那么 $\boldsymbol{m} := \mathrm{col}_j\boldsymbol{B}$；

情况2：如果 $h_{i,i} < \varepsilon$，那么 $\boldsymbol{m} := \mathrm{col}_{n-1}\boldsymbol{B}$；

步骤5：如果 $0 < |\boldsymbol{m}|_{\infty} \leqslant N$，那么转向步骤12；

如果 $|\boldsymbol{m}|_{\infty} > N$，那么不存在这样的整数关系，算法终止；

步骤6：$i := i + 1$；

步骤7：选择整数 r，对 $1 \leqslant j \leqslant n-1$，使得

$$\tau^r |h_{r,r}| \geqslant \tau^j |h_{i,i}|；$$

步骤8：令 $\alpha := h_{r,r}$，$\beta := h_{r+1,r}$，

$$\lambda := h_{r+1,r+1}, \sigma := \sqrt{\beta^2 + \lambda^2}；$$

步骤9：交换 h_r 与 h_{r+1}，定义转置矩阵 $\boldsymbol{R}$；

步骤10：设 $\bar{\boldsymbol{x}} := \bar{\boldsymbol{x}}\cdot\boldsymbol{R}$，$\boldsymbol{H} := \boldsymbol{R}\cdot\boldsymbol{H}$，$\boldsymbol{A} := \boldsymbol{R}\cdot\boldsymbol{A}$，$\boldsymbol{B} := \boldsymbol{B}\cdot\boldsymbol{R}$，如果 $i = n-1$，那么转向步骤4；

步骤11：定义 $\boldsymbol{Q} := (q_{i,j}) \in U(n-1,\mathbb{R})$，$\boldsymbol{H} := \boldsymbol{H}\cdot\boldsymbol{Q}$，转向步骤4；

步骤12：返回 $\boldsymbol{m}$。

从上述3个定理可知，算法1的正确性是显然的。

通过算法1可以找到向量 $\boldsymbol{x} = (1,\tilde{\alpha},\tilde{\alpha}^2,\cdots,\tilde{\alpha}^n)$ 的整数关系，因此可以得到次数为 n 的多项式，令 $G(x) = \boldsymbol{m}\cdot(1,x,x^2,\cdots,x^n)^{\mathrm{T}}$。

在下一部分中，目的是证明在假设误差控制的前提下所得到的多项式 $G(x)$ 是唯一的，同时讨论并给出误差控制 ε 的上界。

2　通过近似值重构极小多项式及新的表示方法

为解答上文中的问题,首先给出一些重要的引理和定理。

引理 1　假设 $f=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$ 是次数为 n 的多项式,令 $\varepsilon=\max_{1\le i\le n}|\alpha^i-\tilde{\alpha}_i|$(在下文中没有特别说明,$\varepsilon$ 的定义依此),其中,对 $1\le i\le n$,$\tilde{\alpha}_i$ 是代数数 α 的 i 次幂的有理近似值,$\tilde{\alpha}_0=1$,那么

$$|f(\alpha)-f(\tilde{\alpha})|\le\varepsilon\cdot n\cdot|f|_\infty。$$

证明:由引理的假设,可得 $f(\alpha)-f(\tilde{\alpha})=\sum_{i=0}^{n}a_i(\alpha^i-\tilde{\alpha}_i)$,因此,

$$|f(\alpha)-f(\tilde{\alpha})|=|\sum_{i=0}^{n}a_i(\alpha^i-\tilde{\alpha}_i)|,$$

那么 $|\sum_{i=1}^{n}a_i(\alpha^i-\tilde{\alpha}_i)|\le\sum_{i=1}^{n}|a_i|\cdot|\alpha^i-\tilde{\alpha}_i|\le\sum_{i=1}^{n}|a_i|\cdot\varepsilon\le n\cdot|f|_\infty\cdot\varepsilon$。证毕。

引理 2[5]　假设 h 和 g 是两个在 $\mathbb{Z}[x]$ 上次数分别为 n 和 m 的非零多项式,如有实数 α 是 h 的根,其中,$|\alpha|<1$,同时如果 h 是不可约的且 $g(\alpha)\neq0$,那么 $|g(\alpha)|\ge n^{-1}\cdot|h|_\infty^{-m}\cdot|g|_\infty^{-n+1}$。

注:如果 $|\alpha|>1$,只需简单的变形即可得到,本文中无特别说明,都假设 $|\alpha|<1$。引理 2 也告诉我们这样的结论:如果 $|g(\alpha)|<n^{-1}\cdot|h|_\infty^{-m}\cdot|g|_\infty^{-n+1}$,那么,$g(\alpha)=0$。

推论 1　假设 h 和 g 是两个在 $\mathbb{Z}[x]$ 上次数分别为 n 和 m 的非零多项式,如有实数 α 是 h 的根,同时如果 h 是不可约的且 $g(\alpha)\neq0$,那么

$$|g(\alpha)|\ge n^{-1}\cdot(n+1)^{-\frac{m}{2}}\cdot(m+1)^{\frac{1-n}{2}}\cdot|h|_\infty^{-m}\cdot|g|_\infty^{-n+1}。$$

证明:首先注意到,对任意次数为 n 的多项式 f 有:$|f|^2\le(n+1)|f|_\infty^2$,因此 $|f|\le\sqrt{n+1}|f|_\infty$。

根据引理 2 整理可得:

$$|g(\alpha)|\ge n^{-1}\cdot(n+1)^{-\frac{m}{2}}\cdot(m+1)^{\frac{1-n}{2}}\cdot|h|_\infty^{-m}\cdot|g|_\infty^{-n+1}。$$

证毕。

定理 4　设 $\tilde{\alpha}$ 是某个次数为 n 代数数 α 的近似值,有次数为 n 多项式 $G(x)=\sum_{i=0}^{n}a_ix^i$。假设已知代数数 α 的极小多项式 $g(x)$ 的高度上界为 N(在下文中没有特别说明,N 的定义依此),如果 $|G(\tilde{\alpha})|<n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}-n\cdot\varepsilon\cdot|G|_\infty$,那么

$$|G(\tilde{\alpha})|<n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}。$$

证明:根据引理 1,注意到 $|G(\alpha)-G(\tilde{\alpha})|\le n\cdot|G|_\infty\cdot\varepsilon$,$|G(\alpha)-G(\tilde{\alpha})|\ge|G(\alpha)|-|G(\tilde{\alpha})|$。因此,$|G(\alpha)|\le|G(\tilde{\alpha})|+n\cdot|G|_\infty\cdot\varepsilon$。定理假设 $|G(\tilde{\alpha})|<n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}-n\cdot\varepsilon\cdot|G|_\infty$,其中,$n\cdot\varepsilon\cdot|G|_\infty>0$,故定理结论显然成立。证毕。

推论 2　设 $\tilde{\alpha}$ 是某个次数为 n 代数数 α 的近似值,如果 $|G(\alpha)|<n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}$,其中,多项式 $G(x)$ 是由改进的带参数的整数关系算法获得,那么 $G(\alpha)=0$,$G(x)$ 的本原部分为代数数 α 的极小多项式。

证明:用反证法。假设 $G(\alpha)\neq0$,根据引理 2,那么 $|G(\alpha)|\ge n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}$。由定理 4,有 $|G(\alpha)|<n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}$,这与假设矛盾,故 $G(\alpha)=0$。假设 $G(x)=\sum_{i=0}^{n}a_ix^i$ 是由向量 $\boldsymbol{v}=(1,\alpha,\alpha^2,\cdots,\alpha^n)$ 调用算法 1 获得,又由推论假设可知,α 为 n 次代数数。根据极小多项式的定义,那么多项式 $G(x)$ 的本原部分是不可约的并且恰好等于 $g(x)$,显然也是唯一的。证毕。

定理 5　设 $\tilde{\alpha}$ 是某个次数为 n 代数数 α 的近似值,如果 $\varepsilon=|\alpha-\tilde{\alpha}|<1/(n^2(n+1)^{n-\frac{1}{2}}N^{2n})$,那么 $G(\alpha)=0$,多项式 $G(x)$ 的本原部分是代数数 α 的极小多项式,其中,多项式 $G(x)$ 是由改进的带参数的整数关系算法获得。

证明:根据定理 4 和推论 2,当且仅当 $|G(\alpha)|<n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}$,那么 $G(\alpha)=0$。在此,不妨设 $\tilde{\alpha}$ 不是 $G(x)=0$ 的根,由 $\tilde{\alpha}$ 是代数数 α 的近似值,那么 $G(\tilde{\alpha})\neq0$,则 $|G(\tilde{\alpha})|>0$。依定理 4 的假设有:$0<n^{-1}\cdot(n+1)^{-n+\frac{1}{2}}\cdot|G|_\infty^{-n}\cdot N^{1-n}-n\cdot\varepsilon\cdot|G|_\infty$,该不等式成立有条件:$\varepsilon<1/(n^2\cdot(n+1)^{n-\frac{1}{2}}\cdot|G|_\infty^{n+1}\cdot N^{n-1})$。又因为 α 为 n 次代数数,再由定理 3 和算法 1 的第 5 步骤可知,$|G|_\infty$ 不超过上界 N,因此这里取 N 代替 $|G|_\infty$。证毕。

基于定理 5 可得通过近似值重构准确结果的算法。

算法2　获得准确极小多项式算法

输入:三元组序列 $(\tilde{\alpha},n,N)$,其中,$\tilde{\alpha}$ 为某个次数为 n 代数数 α 的浮点数满足定理5的误差控制

输出:多项式 $g(x)$,代数数 α 的极小多项式

步骤1:构造向量 $v=(1,\tilde{\alpha},\tilde{\alpha}^2,\cdots,\tilde{\alpha}^n)$;

步骤2:计算 ε 满足定理5;

步骤3:调用算法1获得向量 v 的整数关系 w;

步骤4:获得多项式 $w(x)$;

步骤5:赋予 $g(x)$ 为多项式 $w(x)$ 的本原部分;

步骤6:返回 $g(x)$。

从定理5可知,算法2的正确性是显然的。输入中的三元组序列 $(\tilde{\alpha},n,N)$,将它称为实代数新的准确表示方法,该表示所需要的二进制比特位为 $O(n(\log n+\log N))$。目前,区间方法、符号方法和序方法所需的二进制比特位分别为 $O(n\lg|f|_1+n\lg n))$、$O(n\lg|f|_1+n))$、$O(n\lg|f|_1+\lg n))$。然而,在计算机中引入多项式的存储必将增大它所需的比特位数,尤其是在稠密多项式的情况下,这将是作者提出的新的表示方法的优势。

基于算法2,设计了1个简单的整系数多元多项式因式分解算法。

算法3　整系数多元多项式因式分解算法

步骤1:用 Hilbert 不可约定理将多元多项式约化为2个变元的多项式,基本思想描述见参考文献[16];

步骤2:将约化后的多项式其中1个变元替换为超越数转化为单变元的多项式,实现算法见参考文献[17],通过获取两个变元的多项式的因式,用 Hensel 提升方法获得原多元多项式的因式;

步骤3:通过数值方法获得替换后多项式的近似根,用算法2去获得对应准确根的不可约多项式,那么它一定是给定多项式的因式。

步骤4:重复步骤3,直到所有的因式都找到。算法终止。

3　数值结果

下列例子都是使用 PIV3.0 G,512 M RAM 的机器在 Maple11 的平台上计算出来的。

例1: 已知某个未知代数数 α 的次数 $n=4$ 和它对应的极小多项式的高度 $N=10$,首先根据定理5计算精度控制误差 $\varepsilon=1/(4^2\cdot5^{\frac{7}{2}}\cdot10^8)\approx2.24\times10^{-12}$。然后调用算法2,如果代数数 α 的近似值 $\tilde{\alpha}=0.31783724519578$,只要满足 $|\alpha-\tilde{\alpha}|<\varepsilon$,那么就可以获得它的唯一极小多项式 $g(x)=x^4-10x^2+1$。因此准确的代数数 α 可表示为

$$\langle\alpha\rangle=\langle0.31783724519578,4,10\rangle,$$

即:

$$\langle\sqrt{3}-\sqrt{2}\rangle=\langle0.31783724519578,4,10\rangle。$$

例2: 已知某个未知代数数 α 的次数 $n=2$ 和它对应的极小多项式的高度 $N=25379$,首先根据定理5计算精度控制误差 $\varepsilon=1/(2^2\cdot3^{\frac{3}{2}}\cdot25379^4)\approx1.16\times10^{-19}$。然后调用算法2,如果代数数 α 的近似值 $\tilde{\alpha}=30.146324387756199952819430$,只要满足 $|\alpha-\tilde{\alpha}|<\varepsilon$,那么就可以获得它的唯一极小多项式 $g(x)=6084x^2-11076x-25379$。因此准确的代数数 α 可表示为

$$\langle\alpha\rangle=\langle3.146324387756199952819430,2,25379\rangle,$$

即:

$$\langle\sqrt{5}+71/78\rangle=\langle3.146324387756199952819430,2,25379\rangle。$$

例3: 本例子是算法2在因式分解中的应用。由于考虑方便显示,选择一个很简单的多项式

$$p=5x^9-10x^8+20x^7-40x^6+25x^5+40x^4-30x^3-30x^2+5x+5。$$

通过重构整系数的极小多项式来分解多项式 p。首先将多项式 p 写成首一的形式

$$p=x^9-2x^8+4x^7-8x^6+5x^5+8x^4-6x^3-6x^2+x+1。$$

已知多项式 p 系数的上界为8,由 Landau-Mignotte 界可知它的因式的上界[18]。根据算法3,取 $N=4$,$n=3$,计算 $\varepsilon=1/(3^2\cdot4^{\frac{5}{2}}\cdot4^6)\approx8.48\times10^{-7}$,用 Maple 命令 [fsolve(p=0,x)] 计算多项式的近似根:$S=[-0.4655712319,0.4612542492,1.248321784]$。

根据定理5,取 $\tilde{\alpha}=-0.4655712319$ 是某个次数为3的代数数近似值,调用算法2得到如下多项式

$$p_1=x^3-2x^2+x+1,$$

再用多项式除可得到多项式

$$p_2=x^6+3x^4-3x^3-4x^2+1。$$

由 Eisenstein 判别法[19]知,p_2 是不可约的。因此,p_1 和 p_2 是多项式 p 的因式。

4　总　结

提出了通过近似方法来重构准确极小多项式的算法,算法的核心思想是通过对给定近似值依据定理5给出的误差控制上界,利用改进的带参数的整数关系算法找到了对应准确值的极小多项式,并以此为基础提出了一种新的实代数数计算机表示方法。基于本文的算法,成功地通过重构近似值的极

小多项式获得准确的多项式因式。因此，下一步的工作是研究如何对采用近似方法的实代数的表示进行相应的基本运算和推广到任意代数数的计算机表示，开发基于高效符号数值混合计算系统[20]的程序包，并将本文的算法与思想应用于自动推理、信息安全、程序验证等领域，以解决符号计算中间过程膨胀问题。

参考文献：

[1] Yang L，Zhang J Z，Hou X R. A criterion of dependency between algebraic equations and its applications [C]//Wu W-T，Cheng M-D. Proceeding of International Workshop on Mathematics Mechanization 1992. Beijing：International Academic Publishers，1992：110 - 134.

[2] Zhang J Z，Feng Y. Obtaining exact value by approximate computations [J]. Science in China Series A：Mathematics，2007，50(9)：1361 - 1368.

[3] Zhang J Z，Feng Y，Tang X J. Multivariate polynomial factorization by Interpolation methods (extended abstract) [C]//Pae Sungil，Park H. Proc the 7th Asian Symposium on Computer Mathematics (ASCM2005). Seoul，2005.

[4] Blum M，Micali S. How to generate cryptographically strong sequences of pseudo random bits [C]// Proc 23rd Annual Symposium on Foundations of Computer Science. 1982：112 - 117.

[5] Kannan R，Lenstra A K，Lovász L. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers [J]. Math Comput，1988，50(182)：235 - 250.

[6] Ferguson H R P，Bailey D H，Arno S. Analysis of PSLQ，An integer relation finding algorithm [J]. Math Comput，1999，68(225)：351 - 369.

[7] Mishra B. Algorithmic algebra [M]. New York：Springer-Verlag，1993.

[8] Richtmyer R，Devaney M，Metropolis N. Continued fraction expansions of algebraic number [J]. Numer Math，1962(4)：68 - 84.

[9] Bryuno A D. Continued fraction expansion of algebraic numbers [J]. Comput Math Phys，1964(4)：1 - 15.

[10] Vuillemin J E. Exact real computer arithmetic with continued fractions [J]. IEEE Transactions on Computers，1990，39(8)：1087 - 1105.

[11] Edalat A，Potts P J. A new representation for exact real numbers [J]. Electronic Notes in Theoretical Computer Science，1997(6)：119 - 132.

[12] Zakirov N R. Representation of algebraic numbers by periodic branching continued fractions [J]. Moscow University Mathematics Bulletin，2007，62(4)：24 - 29.

[13] Lang S，Trotter H. Continued fractions of some algebraic numbers [J]. J Reine Angew Math，1972(255)：112 - 134.

[14] Yuan J. An algorithm for continued fractions of algebraic number [J]. Journal of Northwest University：Natural Science Edition，2001，31(1)：1 - 4. [袁进. 一类代数数的连分数表示的一个算法 [J]. 西北大学学报：自然科学版，2001，31(1)：1 - 4.]

[15] Shen J H. Algorithm to compute ordinary continued fractions for a kind of real algebraic numbers [J]. Journal of Tongji University，2001，29(6)：696 - 699. [沈剑华. 一类实代数数的简单连分数展开式的算法 [J]. 同济大学学报，2001，29(6)：696 - 699.]

[16] Corless R M，Galligo A，Kotsireas I S，et al. A geometric-numeric algorithm for absolute factorization of multivariate polynomials [C]//ISSAC'02：Proceedings of the 2002 international symposium on symbolic and algebraic computation. New York，USA：ACM Press，2002：37 - 45.

[17] van der Hulst M-P，Lenstra A K. Factorization of polynomials by transcendental evaluation [C]//Lecture Notes in Computer Science. EUROCAL'85，Berlin：Springer，1985(204)：138 - 145.

[18] Mignotte M. An inequality about factors of polynomials [J]. Math Comp，1974，28(128)：1153 - 1157.

[19] Lang S. Algebra [M]. 3rd Ed. New York：Springer-Verlag，2002.

[20] Qin X L，Feng Y，Li J. Research and design of efficient symbolic and numeric computation system [J]，Computer Engineering and Applications，2009，45(5)：64 - 66. [秦小林，冯勇，李骏. 高效符号数值混合计算系统研究与设计 [J]. 计算机工程与应用，2009，45(5)：64 - 66.]

(编辑　杨　蓓)