软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(3):517−526 [doi: 10.13328/j.cnki.jos.004978]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

有界闭连通域上的非线性循环终止性分析*

李 轶, 冯 勇

(自动推理与认知重庆市重点实验室(中国科学院 重庆绿色智能技术研究院),重庆 401120)

通讯作者: 李轶, E-mail: zm_liyi@163.com

摘 要: 运用计算机代数中的 Groebner 基理论,对有界闭连通域上的单重非线性循环程序的终止性问题进行研究,建立了可计算的终止性判定算法.该算法将这类循环的终止性判定问题归约为有无不动点的判定问题.

关键词: 可信计算;非线性循环;终止性分析;Groebner 基;计算机代数

中图法分类号: TP301

中文引用格式: 李轶,冯勇.有界闭连通域上的非线性循环终止性分析.软件学报,2016,27(3):517−526. http://www.jos.org.cn/1000-9825/4978.htm

英文引用格式: Li Y, Feng Y. Termination analysis of non-linear loops over closed and bounded connected domain. Ruan Jian Xue Bao/Journal of Software, 2016,27(3):517−526 (in Chinese). http://www.jos.org.cn/1000-9825/4978.htm

Termination Analysis of Non-Linear Loops over Closed and Bounded Connected Domain

LI Yi, FENG Yong

(Chongqing Key Laboratory of Automated Reasoning and Cognition (Automated Reasoning and Cognition Center, Chongqing Institute of Green and Intelligent Technology, The Chinese Academy of Sciences), Chongqing 401120, China)

Abstract: Termination of a class of nonlinear loops is analyzed in this paper. Based on Groebner bases, determining the termination problem of this type of loop programs is equivalent to determining whether or not the iteration functions of the loops have fixed points in the domains specified by loop guards.

Key words: trusted computing; non-linear loop; termination analysis; Groebner base; computer algebra

随着信息技术的迅猛发展,嵌入式系统在人类生活中发挥着越来越大的作用,嵌入式软件在其中所占有的比重也越来越大.因此,嵌入式软件的可靠性将变得更加重要.诸如航空、航天、军事、交通、医疗等关键应用领域都对嵌入式系统的可靠性和安全性要求非常高,任何错误的发生都可能带来灾难性后果.这些系统被称为攸关安全系统.

嵌入式系统具有 3 个重要属性,即可达性、终止性、不变式.可达性是指系统能否从给定状态到达另一个可接受状态,某些混成系统的可达性被证明是能用计算机代数工具来检验的;不变式则是用于描述在程序运行时保持函数不变性质的逻辑断言;而终止性是研究系统中是否会发生死循环,不包括终止性分析的验证被称为程序的部分正确性证明.因此,程序的终止性分析是确保程序完全正确性的必要基础.

尽管程序的终止性问题早已被证明是不可判定的[12],但对其进行研究不仅具有理论意义,更具有实际意义.当前,国际上主要通过合成秩函数来进行循环终止性分析,并取得了一些突破.例如,Poldelski 等人[15]基于线性代数理论提出了完备的一类线性程序线性秩函数生成理论,并开发出工具 RANKFINDER,该工具是他们与微软联合开发的程序终止性分析工具 TERMINATOR 的核心部分[1].此外,利用 Farkas 引理及多面体理论,针对这

* 基金项目: 国家自然科学基金(61572024, 61103110, 11171053)
Foundation item: National Natural Science Foundation of China (61572024, 61103110, 11171053)
收稿时间: 2015-07-02; 修改时间: 2015-10-20; 采用时间: 2015-11-27; jos 在线出版时间: 2016-01-05
CNKI 网络优先出版: 2016-01-05 16:39:44, http://www.cnki.net/kcms/detail/11.2560.TP.20160105.1639.001.html

类线性循环程序,文献[10,11]呈现了线性秩函数合成算法.最近,文献[4]研究了现有几种秩函数生成算法的时间复杂度.在 2013 年,文献[5]进一步分析了程序变量在整数集合上取值时,这类线性程序的线性秩函数合成方法,并研究了这类问题的复杂度.

近年来,计算机代数和实代数理论已逐渐被应用于程序自动验证.例如,我国科学家杨路、夏壁灿、詹乃军和周巢尘等人将秩函数和不变式的计算归约为半代数系统的求解,并运用实代数工具 DISCOVERER 提出了多项式不等式型不变式和非线性秩函数生成方法[9,20].不同于文献[14]中的方法,他们的方法能够精确回答循环程序是否有给定模板的秩函数或不变式.合成秩函数是验证循环程序终止性的一条重要途径,但是秩函数的存在是循环可终止的充分而非必要条件[5,7].人们容易构造一个循环程序,它是可终止的,但并没有秩函数.此外,文献[8,13]提出了试探性方法去探索给定循环程序的非终止性,对可终止的循环程序,他们的方法不再适用.尽管众所周知,一般的程序终止性问题是不可判定的,但对特定的一类程序而言,人们总希望能证明其终止性问题是可判定的.由此,证明循环程序终止性的另一途径就是避开秩函数的合成,而采用数学方法严格证明某类或某些类循环程序的终止性是可判定的,并建立相对完备的判定算法.目前,从可判定的角度进行终止性研究的结果甚少.在 2004 年,Tiwari 在文献[16]中首次证明了一类单重无分支线性循环程序在实域上的终止性是可判定的.相似的结论被 Braveman[7]推广到整数环上.此外,为避免 Jordan 标准型的浮点计算,文献[17]中提出了精确的符号计算方法对这类线性程序进行终止性判定.既然一般形式的线性程序终止性是不可判定的[16],那么非线性循环程序由于其更为复杂的动力行为使得其终止性分析将变得更加困难.一个程序被称为非线性的,是指循环中的赋值映射或循环条件中的约束是非线性表达式.在 2005 年,利用有限差分树理论,文献[6]提出了试探性算法对一类含多分支语句的多项式程序的终止性问题进行判定.2010 年,针对一类赋值为线性且循环条件由非线性多项式不等式构成的循环程序,文献[18]分析了其终止性问题,证明了当这类程序满足给定的 NZM 条件时,其终止性是可判定的.2013 年,文献[3]通过分析多项式映射 f_i 的发散区间,讨论了一类多项式循环(迭代赋值型如 $x_i:=f_i(x_i)$)的终止性问题.

本文中,我们对赋值映射 F 为非线性、循环条件形成有界闭连通域 S 的一类非线性循环程序 $\mathbf{P}(F,S)$的终止性问题进行了分析.不同于文献[6],本文呈现的方法并不依赖于有限差分树理论.同时,本文所研究的程序类型是文献[3,7,16–18]中的程序类型的扩展.我们给出了适当的条件,证明了当循环程序满足这些条件时,这类循环程序在实域上可终止的充分必要条件为迭代映射 F 在有界闭连通域 S 上没有不动点.同时,对任给的连续迭代映射 F,本文建立的引理 1,便于我们分析当其有界闭连通域 S 取自哪个区域时,可使得 F 在该 S 上进行的迭代是可终止的.我们的算法依赖于计算机代数中的 Groebner 基理论和半代数系统求解,因此,计算机代数工具 DISCOVERER[2,19],BOTTEMA[2]以及 Maple 在算法中被运用.

1 主要结果

第 1.1 节,针对赋值映射 F 为连续的且 S 为有界闭连通域的循环程序,建立了相关终止性的一般性结论,将其终止性问题规约为:在满足一定条件下,迭代映射有无不动点的判定问题;但验证所需的前提条件是否被满足,则是需要讨论的问题.因此在第 1.2 节中,我们进一步限制 F 为多项式映射,然后给出方法去验证所需的前提条件是否成立.

1.1 有界闭连通域上的循环终止性分析

本节中,我们对循环条件围成的区域 S 为有界闭连通域、赋值映射 F 为非线性连续映射的循环程序终止性问题进行分析.这里,我们设置 S 为有界闭的,是因为物理世界中的诸多变量,如速度、加速度等都是有界的量;而闭性的限制则是为了保证收敛序列的极限点能落到 S 中.这类循环程序被称为是不可终止的,如果存在一点 $X^*\in R$,使得对任意的非负整数 k,有 $F^k(X^*)\in S$.如果这样的点不存在,则称这类循环在实数域上是可终止的.这里,

$$F^k=\underbrace{F\circ F\circ\ldots\circ F}_{k}.$$

首先,我们给出引理 1:

引理 1. 设 S 是 n 维空间中的有界闭的连通域,给定 n 维连续映射 $F:X|\to F(X)$.如果循环程序:

$$\begin{array}{c}\textbf{while } X\in S \textbf{ do}\\ \{X=F(X)\}\\ \textbf{endwhile}\end{array}\tag{1}$$

在 S 上不可终止,则对任意正整数 k,集合 $\{X\in R^n:|F^k(X)=|X|\}$ 与 S 均相交(这里,$|\circ|$ 表示向量 $\circ$ 的欧式范数).

证明:若上述循环程序在 S 上不可终止,则必存在一个点 $X\in S$,生成无穷点列:

$$\Delta=\{X_0,F(X_0),F^2(X_0),\ldots\}\subseteq S.$$

记 $r_\perp=\textbf{sup}\{|F^n(X_0)|\}_{n=0}^{\infty}, r_\top=\textbf{inf}\{|F^n(X_0)|\}_{n=0}^{\infty}$.令 $|\Delta|=\{|F^n(X_0)|\}_{n=0}^{\infty}=\{r_n\}_{n=0}^{\infty}$.下面证明 k=1 时定理成立,k=2,3,…时的证明完全类似.

我们首先证明,分别存在两点 $X_\perp\in\{X\in R^n:|X|=r_\perp\}\cap S, X_\top\in\{X\in R^n:|X|=r_\top\}\cap S$,使得:

$$|F(X_\perp)|\leqslant|X_\perp|,|F(X_\top)|\geqslant|X_\top|.$$

我们仅证明 $|F(X_\perp)|\leqslant|X_\perp|,|F(X_\top)|\geqslant|X_\top|$ 的证明类似.

首先,若 $r_\perp\in|\Delta|$,不妨记为 $r_\perp=|F^t(X_0)|=|X_t|$,则显然有 $|F(X_t)|\leqslant|X_t|=r_\perp$,令 $X_\perp=X_t$;倘若 $r_\perp\notin|\Delta|$,既然 Δ 为有界数列,则由确界性质,必存在 $|\Delta|$ 的子列 $\{r_{n_k}\}$ 收敛于 $r_\perp$,即 $\lim_{k\to\infty}r_{n_k}=r_\perp$.既然 $F^{n_k}(X_0)=X_{n_k}=r_{n_k}(\eta_{n_k}^{(1)},\eta_{n_k}^{(2)},...,\eta_{n_k}^{(n)})^T$,令:

$$\eta_{n_k}=(\eta_{n_k}^{(1)},\eta_{n_k}^{(2)},...,\eta_{n_k}^{(n)})^T,|\eta_{n_k}|=1.$$

显然,数列 $\{\eta_{n_k}\}_{k=0}^{\infty}$ 是有界的.根据 Bolzano-Weierstrass 定理可知,R^n 上的有界数列必有收敛子列.因此,存在 $\{\eta_{n_k}\}$ 的子列 $\{\eta_{n_{k_v}}\}$,有:

$$\lim_{v\to\infty}\eta_{n_{k_v}}=\eta^*.$$

又因为 $\lim_{k\to\infty}r_{n_k}=r_\perp$,故其任意收敛子列也收敛于 $r_\perp$,因此有:

$$\lim_{v\to\infty}r_{n_{k_v}}\eta_{n_{k_v}}=r_\perp\eta^*.$$

因此,在 Δ 中存在子列 $\{F^{n_{k_v}}(X_0)\}_{v=0}^{\infty}$,使得 $\lim_{v\to\infty}F^{n_{k_v}}(X_0)=r_\perp\eta^*$.令 $X_\perp=r_\perp\eta^*$.

既然 $\Delta\subseteq S$,则 $X_\perp\in\{X\in R^n:|X|=r_\perp\}\cap S$.

又因为 $r_\perp\notin|\Delta|$ 且为 $|\Delta|$ 上确界,则 $|F(F^{n_{k_v}}(X_0))|<|X_\perp|=r_\perp$.两边取极限,由 F 的连续性,

$$\lim_{v\to\infty}|F(F^{n_{k_v}}(X_0))|=|F(\lim_{v\to\infty}F^{n_{k_v}}(X_0))|=|F(X_\perp)|\leqslant|X_\perp|=r_\perp.$$

同理可证:存在 $X_\top\in\{X\in R^n:|X|=r_\top\}\cap S$,有 $|F(X_\top)|\geqslant|X_\top|$.记 $G=|F(X)|-|X|$.既然存在两点 $X_\perp,X_\top\in S$,使得 $G(X_\perp)\leqslant 0, G(X_\top)\geqslant 0$,若上述两式其中一个等号成立,则令 $X^*=X_\perp$(或 $X_\top$),有 $G(X^*)=0$.因此不失一般性,假设两式中的等号都不成立,则根据多元连续函数在有界闭集上的性质可知:必存在一点 $X^*\in L(X_\perp,X_\top)$,使得 $G(X^*)=0$.这里,$L(X_\perp,X_\top)\in S$ 为 S 中连接 $X_\perp,X_\top$ 两点的一条折线.因此,集合 $\{X\in R^n:|F(X)=|X|\}$ 与 S 必相交.

同样地,将上述证明中 F 改为 F^k,k=2,3,…,采用类似的方法可证明:存在两点 $X_\perp\in\{X\in R^n:|X|=r_\perp\}\cap S$, $X_\top\in\{X\in R^n:|X|=r_\top\}\cap S$,使得 $|F^k(X_\perp)|\leqslant|X_\perp|,|F^k(X_\top)|\geqslant|X_\top|$,$k$=2,3,…,进而可证 $\{X\in R^n:|F^k(X)=|X|\}$ 与 S 必相交. □

注:根据上述定理,倘若存在正整数 k 使得 $|F^k(X)|=|X|$ 与 S 不相交,则该循环程序在 S 上可终止.实际上,既然 $|F^k(X)|=|X|$ 等价于 $|F^k(X)|^2=|X|^2$,故若存在正整数 k 使得 $|F^k(X)|^2=|X|^2$ 与 S 不相交,则该循环程序在 S 上可终止.这样,在实际的计算中可避免根号的处理.

根据引理 1,给定迭代映射 F,我们可以确定:当 S 取自哪些区域时,形如公式(1)的循环程序是可终止的.为方便起见,这样的区域称为安全区域.

例 1:考虑使得下列循环可终止的安全区域.

$$\begin{array}{l}\textbf{while } x\in S \textbf{ do}\\ x:=xy+2x^2+y+1\\ y:=x-y^2+y-5\\ \textbf{endwhile}\end{array} \tag{2}$$

令 $F=(f_1,f_2)^T=(xy+2x^2+y+1,x-y^2+y-5)^T$.作 $T_k(x,y)=|F^k(X)|^2-|X|^2$.令 $\Theta_k=R^n-\{(x,y)\in R^2:T_k(x,y)=0\}$.因此,对固定的 k,则 Θ_k 中的任意有界闭域都是该循环的安全区域.如在此例中,倘若令 $k=1,S=\{x^2-y\geqslant 1,y\geqslant 2,x\leqslant 7\}$,因为 $S\cap T_k(x,y)=\varnothing$,则 F 在 S 上的迭代可终止.即,这样设置的 S 是循环(2)的一个安全区域.

引理 1 为循环(1)的可终止性提供了充分判准.首先给出下面一类特殊的循环,根据引理 1 可知,其终止性与不动点有着紧密的联系.

令 $R_+^n=\{(x_1,...,x_n)\in R^n:x_i>0,i=1,...,n\},S_+\subset R_+^n$ 为有界闭连通域.令 $\hat{F}(X)$ 为多项式映射,即:

$$\hat{F}(X)=(f_1,f_2,...,f_n)^T,f_i\in R[X]且f_i=c_ix_i+\sum_\alpha c_\alpha X^\alpha(X^\alpha=x_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}),$$

其中,$c_i\geqslant 1,c_\alpha>0$.通常称 x_i 为多项式 f_i 的导元.因此,$\hat{F}$ 中每个 f_i 均含有其导元的线性项,且该项的系数大于等于 1,而其余项系数均为正数,譬如 $\hat{F}=(x_1+x_1x_2+4x_2^2,3x_2+7x_1+2)^T$.给定型如下列类型的循环程序(3):

$$\begin{array}{l}\textbf{while } X\in S_+ \textbf{ do}\\ \{X=\hat{F}(X)\}\\ \textbf{endwhile}\end{array} \tag{3}$$

则根据引理 1,可建立下列结果.

定理 2. 记号同上.循环程序(3)不可终止的充分必要条件是 $\hat{F}$ 在 S_+上有不动点.

证明:倘若 $\hat{F}$ 在 S_+上有不动点,则循环程序(3)显然不可终止.因此,下面仅证明当 $\hat{F}$ 在 S_+上没有不动点时,循环程序(3)是可终止的.既然 $|\hat{F}(X)|^2-|X|^2=\sum_{i=1}^n f_i^2-\sum_{i=1}^n x_i^2$,

$$\sum_{i=1}^n f_i^2-\sum_{i=1}^n x_i^2=\sum_{i=1}^n(f_i-x_i)^2+2\sum_{i=1}^n x_if_i-2\sum_{i=1}^n x_i^2=\sum_{i=1}^n(f_i-x_i)^2+2\sum_{i=1}^n(x_i(f_i-x_i)).$$

根据已知,$\hat{F}$ 在 S_+上没有不动点,因此对任意的 $X\in S_+$,有 $\sum_{i=1}^n(f_i(X)-x_i)^2>0$.同时,根据 $\hat{F}$ 的构造可知(即,每个 f_i 均含有其导元的线性项,且该项的系数大于等于 1),$x_i(f_i-x_i)$在 S_+上非负,因此,$\sum_{i=1}^n f_i^2-(\sum_{i=1}^n x_i^2)$ 在 S_+上恒为正.故对任意的 $X\in S_+,|\hat{F}(X)|^2\neq|X|^2$.也即:对任意的 $X\in S_+,|\hat{F}(X)|\neq|X|$.

根据引理 1,循环程序(3)是可终止的. □

针对如式(3)的一类特殊循环程序,根据定理 2,我们将这类程序的终止性问题归约为有无不动点的判定,从而使得该类特殊程序的终止性变得便于分析.通过定理 4 可知:利用不动点来分析循环终止性的方法不仅适用于循环(3),在一定条件下,这种方法对更加一般类型的循环(1)仍然适用.我们首先给出下列引理,其中的 S,F 的定义同引理 1.

给定正整数 N,令 $\Gamma_N(X)=\sum_{k=1}^N||F^k(X)|^2-|X|^2|$,令

$$V_R(\Gamma_N(X))=\{X\in R^n:\Gamma_N(X)=0\}=\{X\in R^n:|F(X)|^2-|X|^2=0,...,|F^N(X)|^2-|X|^2=0\},$$
$$V_R(F-X)=\{X\in R^n:F(X)=X\},$$

令 $V_C(\Gamma_N(X))=\{X\in C^n:|F(X)|^2-|X|^2=0,\ldots,|F^N(X)|^2-|X|^2=0\},V_C(F-X)=\{X\in C^n:F(X)=X\}$.

这里,R,C 分别表示实数域和复数域.在给出本文的主要定理前,我们需要下面的引理.

引理 3. 记号同上.假设存在正整数 N,使得 $V_R(\Gamma_N(X))=V_R(F-X)$.那么如果 F 在 S 上没有不动点,则必存在常数 $\nu>0$,使得对任意的 $X\in S$,有:

$$\sum_{k=1}^N||F^k(X)|^2-|X|^2|\geqslant\nu\cdot|F(X)-X|.$$

证明:根据题设 F 在 S 上没有不动点,即:对任意的 $X\in S,|F(X)-X|\neq 0$.又因为 $V_R(\Gamma_N(X))=V_R(F-X)$,故对任意的

$X\in S,\Gamma_N(X)\neq 0$.也即:对任意的 $X\in S,X\notin V_R(\Gamma_N(X))$.

因此,对任意的 $X^*\in S$,必然存在正数 $\nu(X^*)$,使得 $\Gamma_N(X^*)\geqslant \nu(X^*)\cdot|F(X^*)-X^*|$.

又因为函数 $\Gamma_N(X),|F(X)-X|$ 均是连续的(因为 F 是连续的),故根据连续性,必存在 X^* 的开邻域 $O(X^*,\varepsilon)$,使得对任意的 $X\in O(X^*,\varepsilon)$,有 $\Gamma_N(X^*)\geqslant \nu(X^*)\cdot|F(X^*)-X^*|$.由 X^* 的任意性以及 S 有界闭性,存在无穷个开邻域覆盖有界闭连通域 S.由有限开覆盖定理,存在有限个开邻域 $O(X_1^*,\varepsilon_1),O(X_2^*,\varepsilon_2),O(X_3^*,\varepsilon_3),...,O(X_t^*,\varepsilon_t)$ 覆盖 S,即:

$$S\subseteq\bigcup_{i=1}^{t}O(X_i^*,\varepsilon_i).$$

令 $\nu=\min\{\nu(X_1^*),\nu(X_2^*),...,\nu(X_t^*)\}$,则根据上述分析有:

$$\sum_{k=1}^{N}\|F^k(X)|^2-|X|^2|\geqslant\nu\cdot|F(X)-X|. \qquad \square$$

根据引理 1 和引理 3,我们可以建立如下结果.首先,令 $\overline{[1,N]}=\{1,2,3,...,N\}$.

定理 4. 设 S 是 n 维空间中的有界闭的连通域.给定 n 维连续映射 $F:X|\to F(X)$.如果满足:

(i) 存在正整数 N,使得 $V_R(\Gamma_N(X))=V_R(F-X)$;

(ii) 存在 $j\in\overline{[1,N]}$ 和正数 $\hbar$,使得对任意的 $k\in\overline{[1,N]},k\neq j$,有:

$$||F^j(X)|^2-|X|^2|\geqslant\hbar\cdot||F^k(X)|^2-|X|^2|(X\in S),$$

则循环程序(1)在 S 上是不可终止的充分必要条件为:迭代映射 F 在 S 中有不动点.

证明:倘若 F 在 S 中有不动点,则循环程序(1)显然是不可终止的.因此,仅需证明:若 F 在 S 中没有不动点,则循环(1)可终止.既然假设 $V_R(\Gamma_N(X))=V_R(F(X)-X)$ 成立,根据引理 3,若 F 在 S 上没有不动点,则存在正数 ν,使得对任意的 $X\in S,\sum_{k=1}^{N}\|F^k(X)|^2-|X|^2|\geqslant\nu\cdot|F(X)-X|$.根据假设(ii)得知:对任意的 $X\in S$,

$$\left(1+(N-1)\frac{1}{\hbar}\right)\|F^j(X)|^2-|X|^2|\geqslant\sum_{k=1}^{N}\|F^k(X)|^2-|X|^2|\geqslant\nu\cdot|F(X)-X|.$$

又因为 F 在 S 中没有不动点,则 $|F(X)-X|\neq 0$.故 $||F^j(X)|^2-|X|^2|\neq 0(\forall X\in S)$.根据引理 1 可知,循环(1)必然终止. □

定理 4 说明:在满足给定的假设(i)、假设(ii)时,循环程序(1)的终止性可归为在 S 中有无不动点的判定.因此,关键问题是验证假设(i)、假设(ii)是否成立.一般地,因为 F 的任意性,假设(i)的验证是困难的,但是当映射 $F=(f_1,f_2,...,f_n)^T$ 中的每个分量 f_i 都是多项式时,即 F 为多项式映射,我们可将数域从实数域拓展到复数域,从而使得我们可利用多项式代数中的相关理论和工具去判定假设(i)是否成立.即:判定是否存在 N,使得 $V_C(\Gamma_N(X))=V_C(F(X)-X)$ 成立.这是因为,若 $V_C(\Gamma_N(X))=V_C(F(X)-X)$,则 $V_R(\Gamma_N(X))=V_R(F(X)-X)$.而验证假设(ii)是否成立可转换为不等式证明问题,后者可使用杨路等人开发的不等式证明器 BOTTEMA[2]进行验证.因此在下一节中,我们将着重讨论当 F 为多项式映射的循环终止性问题,这类循环被称为多项式循环程序.

1.2 迭代映射为多项式映射

根据定理 4,当迭代映射 F 为连续的循环程序满足两个假设条件(i)、假设(ii)时,其终止性判定问题可转为有无不动点的判定.本节中,我们限定循环(1)中的迭代映射 F 为多项式的,因此 F 必是连续的.既然定理 4 中的假设条件(ii)可用工具 BOTTEMA 予以验证,因此在本节,针对这类多项式循环程序,我们着重分析如何对定理 4 中的假设条件(i)进行验证的问题,并给出了可计算的验证方法.由于需要用到多项式代数的相关理论,如理想、Groebner 基等,因此首先给出一些基本概念.

定义 5[22]. 令 $R[X]$ 为多项式环.子集 $I\subset R[X]$ 被称为一个多项式理想,如果 I 满足以下条件:

(1) $0\in I$;

(2) 若 $a,b\in I$,则 $a+b\in I$;

(3) 若 $a\in I,b\in R[X]$,则 $b\cdot a\in I$.

任给 $N(N\leqslant+\infty)$ 个多项式 $p_1,p_2,...,p_N\in R[X]$,可构建一个多项式理想 $I=\langle p_1,p_2,...,p_N\rangle$.多项式 $p_1,p_2,...,p_N$ 称为理想 I 的一组生成元.称多项式 $a\in I$,如果存在多项式 $q_1,...,q_s\in R[X]$ 和多项式 $f_1,...,f_s\in I$,使得 $a=\sum_{i=1}^{s}q_if_i$.我们称理想 $I_1\subseteq I_2$,如果对任意的元素 $a\in I_1$,都有 $a\in I_2$.任意多项式理想 I,在给定项序下,都有一组具有良好性质的生成元—

一约化 Groebner 基,记为 G.显然,$\langle G\rangle=I$.给定一个理想,根据约化 Groebner 基的性质,可以判定任意多项式 a 是否属于这个理想.令 $V_C(I)=\{X\in C^n:p_i(X)=0,\forall i=1,2,\ldots,N\}$ 为理想 I 的零点集.若 $I_1=I_2$,则 $V_C(I_1)=V_C(I_2)$;若 $I_1\subseteq I_2$,则 $V_C(I_1)\supseteq V_C(I_2)$;若 $I_1=\langle f_1,\ldots,f_s\rangle, I_2=\langle g_1,\ldots,g_t\rangle$,则 $I_1\cup I_2=\langle f_1,\ldots,f_s,g_1,\ldots,g_t\rangle$.有关多项式理想及 Groebner 基的详细介绍见文献[22].譬如,令理想 $I=\langle p_1,p_2\rangle=\langle xz-y^2,x^3-z^2\rangle\in R[X]$.给定多项式 $f=-4x^2y^2z^2+y^6+3z^3$,判定在分级字典序下是否有 $f\in I$?使用计算机代数系统 Maple,可找到理想 I 的约化 Groebner 基.

$$G=(p_1,p_2,p_3,p_4,p_5)=(xz-y^2,x^3-z^2,x^2y^2-z^3,xy^4-z^4,y^6-z^5).$$

根据 G,可通过理想成员测试算法得到:

$$f=(-4xy^2z-4y^4)\cdot p_1+0\cdot p_2+0\cdot p_3+0\cdot p_4+(-3)\cdot p_5.$$

因此,$f\in\langle G\rangle=I$.另外,给定两个多项式理想 I_1,I_2,我们也可以通过计算其各自的约化 Groebner 基 G_1,G_2 来判定是否 $I_1=I_2$,这是因为 $G_1=G_2$ 当且仅当 $I_1=I_2$.

定理 6[22]. 假设 $I_1\subset I_2\subset I_3\subset\ldots\subseteq R[X]$是一组理想升链,则存在正整数 N,使得对任意 $n\geqslant N$ 都有 $I_n=I_{n+1}=I_{n+2}=\ldots$.

根据定理 6,一组理想升链必在某个 N 处达到稳定.等价地,这组理想升链的零点集也在 N 处达到稳定.也即:

$$V_C(I_1)\supset V_C(I_2)\supset\ldots\supset V_C(I_{N^*})=V_C(I_{N^*+1})=\ldots$$

在本文的具体问题中,令 $I_i=\langle|F(X)|^2-|X|^2,|F^2(X)|^2-|X|^2,\ldots,|F^i(X)|^2-|X|^2\rangle$为多项式理想,显然有 $I_i\subseteq I_{i+1}$.通过定理 6 可知:必存在正整数 N^*,使得 $I_{N^*}=I_{N^*+1}$.

命题 7. 给定多项式映射 F,令 $I_i=\langle|F(X)|^2-|X|^2,|F^2(X)|^2-|X|^2,\ldots,|F^i(X)|^2-|X|^2\rangle$为多项式理想,则必存在正整数 N^*,使得 $I_{N^*}=I_{N^*+1}$.

证明:这是显然的.根据 I_i 的构造可知,$I_i\subseteq I_{i+1}$(这是因为理想 I_{i+1} 的生成元比理想 I_i 多出一个生成元$|F^{i+1}(X)|^2-|X|^2$).假设使得 $I_{N^*}=I_{N^*+1}$ 成立的 N^*不存在,则这些理想将形成一条严格升链 $I_1\subsetneq I_2\subsetneq I_3\subsetneq\ldots$,那么根据定理 6,必存在 N^*,使得 $I_{N^*}=I_{N^*+1}$.故假设不成立. □

根据命题 7,使得 $I_{N^*}=I_{N^*+1}$ 的正整数 N^*必定存在.而下面的算法 1 可计算出 N^*.

算法 1.

输入:给定 n 维多项式映射 $F:X|\to F(X)$;

输出:N^*.

S1. 构建理想 $I_i=\langle|F(X)|^2-|X|^2,|F^2(X)|^2-|X|^2,\ldots,|F^i(X)|^2-|X|^2\rangle$;

S2. 如果 $I_i\neq I_i\cup\langle|F^{i+1}(X)|^2-|X|^2\rangle$,则转 S3;否则,转 S4;

S3. $I_i\leftarrow I_i\cup\langle|F^{i+1}(X)|^2-|X|^2\rangle$,转 S2;

S4. 返回 $N^*=i$.

由命题 7 可知,算法 1 显然有限终止.在算法 1 中,两个理想是否相等等价于它们的约化 Groebner 基是否相等.因此,可调用 Maple 中的命令函数计算各自的约化 Groebner 基.既然根据算法 1 可以得到 N^*,可构建 $I_{N^*}=\langle|F(X)|^2-|X|^2,|F^2(X)|^2-|X|^2,\ldots,|F^{N^*}(X)|^2-|X|^2\rangle$.另外,根据 $\Gamma_{N^*}(X)$ 的定义,显然有:

$$V_C(I_{N^*})=V_C(\Gamma_{N^*}(X)).$$

因此,要判定 $V_C(\Gamma_{N^*}(X))=V_C(F(X)-X)$ 是否成立,等价于判定 $V_C(I_{N^*})=V_C(F(X)-X)$.由此,根据算法 2,我们可以判定 $V_C(\Gamma_{N^*}(X))=V_C(F(X)-X)$ 是否成立.

算法 2.

输入:$I_{N^*},F(X)-X=(f_1-x_1,\ldots,f_n-x_n)^T$;

输出:T(相等),F(不相等).

S1. 计算理想 I_{N^*} 的约化 Groebner 基 G_{N^*};

S2. 如果对任意的 i=1,2,…,n,均有 $f_i-x_i\in G_{N^*}$,则返回 T;否则,返回 F.

命题 8. 若算法 2 返回 T,则必有 $V_C(\Gamma_{N^*}(X))=V_C(F(X)-X)$.

证明:根据题设,若算法 2 返回 T,则表明对任意的 i,有 $f_i - x_i \in G_{N^*}$,也即 $f_i - x_i \in I_{N^*}$,这是因为 $\langle G_{N^*}\rangle = I_{N^*}$. 因此,理想 $\langle F(X)-X\rangle = \langle f_1 - x_1,...,f_n - x_n\rangle \subseteq I_{N^*}$. 故 $V_C(F(X)-X) \supseteq V_C(I_{N^*})$.又因为 $V_C(\Gamma_{N^*}(X)) = V_C(I_{N^*})$, 有:

$$V_C(F(X)-X) \supseteq V_C(\Gamma_{N^*}(X)).$$

同时,又因为 $V_C(F(X)-X) \subseteq V_C(\Gamma_{N^*}(X))$,故 $V_C(F(X)-X) = V_C(\Gamma_{N^*}(X))$. □

根据命题 8,若算法 2 返回 T,则 $V_C(\Gamma_{N^*}(X)) = V_C(F-X)$,故 $V_R(\Gamma_{N^*}(X)) = V_R(F(X)-X)$, 满足定理 4 的题设. 此时,循环程序(1)是否可终止的问题等价于 F 在 S 中有无不动点的问题.因此,我们有下列的结论.

定理 9. 设 S 是 n 维空间中的有界闭的连通域.给定 n 维多项式映射 $F:X|\to F(X)$,令:

$$I_i=\langle |F(X)|^2-|X|^2,|F^2(X)|^2-|X|^2,\ldots,|F^i(X)|^2-|X|^2\rangle.$$

如果同时满足:

(i) 存在正整数 N^*,使得 $I_{N^*} = I_{N^*+1}$ 且 $V_C(I_{N^*}) = V_C(F(X)-X)$;

(ii) 存在 $j \in \overline{[1,N^*]}$ 和正数 $\hbar$,使得 $\forall X \in S, \| F^j(X)|^2 - |X|^2| \geqslant \hbar \cdot \| F^k(X)|^2 - |X|^2| \ (\forall k \in \overline{[1,N^*]}, k \neq j)$.

则循环程序(1)在 S 上是不可终止的当且仅当 F 在 S 中有不动点.

证明:因为 $V_C(I_{N^*}) = V_C(\Gamma_{N^*}(X)), V_C(I_{N^*}) = V_C(F(X)-X)$,从而有 $V_C(\Gamma_{N^*}(X)) = V_C(F(X)-X)$,故有:

$$V_R(\Gamma_{N^*}(X)) = V_R(F(X)-X).$$

因此,定理 4 中的假设均成立.由定理 4,结论显然成立. □

注:当 F 为多项式映射时,算法 1 和算法 2 给出了可计算的方法去验证定理 9 中的假设(i)是否成立.而假设(ii)中,判定是否存在正数 $\hbar$,使得 $\forall X \in S, ||F^j(X)|^2-|X|^2| \geqslant \hbar \cdot ||F^k(X)|^2-|X|^2|$ 可以等价转化为存在正数 $\hbar$,使得下列半代数系统:

$$S \cap \{X \in R^n : ||F^j(X)|^2-|X|^2| < \hbar \cdot ||F^k(X)|^2-|X|^2|\}$$

无实解.后者可用 Collins 早期提出的基于柱形代数分解[21]的实量词消去技术进行判定,因而也是可计算的.已有多种实量词消去的工具,如 QEPCAD,Redlog,DISCOVERER,BOTTEMA,RegularChains 等.本文中,我们主要利用工具 BOTTEMA,DISCOVERER 来进行计算.进而,当定理 9 中的两个假设条件都被满足时,则这类多项式循环程序的终止性问题可归结为有无不动点的判定问题.而后者的判定是简单的,这是因为判定 F 是否在 S 中有不动点,等价于计算下列半代数系统:$\{X \in R^n : F(X)-X=0\} \cap S$ 是否非空:若非空,则表明 F 在 S 中有不动点;否则,在 S 上没有不动点.而一个半代数系统是否为空的判定问题等价于实量词消去问题,因而适合运用计算机代数工具 DISCOVERER 予以求解.

根据定理 9,我们给出本文的主要算法,描述如下.

算法 3.

输入:形如(1)的循环程序 P;

输出:True(终止),False(不终止),ND(不确定).

S1. 从循环程序 P 中抽取迭代映射 F,循环条件形成的区域 S,转 S2;

S2. 调用算法 1 计算出正整数 N^*,转 S3;

S3. 调用算法 2 判定 $V_C(I_{N^*}) = V_C(F(X)-X)$ 是否成立:若成立,则转 S4;否则,输出 ND;

S4. 利用工具 BOTTEMA 判定定理 9 中的条件(ii)是否成立:若成立,则转 S5;否则,输出 ND;

S5. 利用工具 DISCOVERER 判定半代数系统 $\{X \in R^n : F(X)-X=0\} \cap S$ 是否有解:若有解,则输出 false;否则,输出 true.

在算法 3 中,S3 和 S4 分别判定定理 9 中的两个前提条件(i)、条件(ii)是否都满足:倘若其中某个条件不满足,那么输出 ND;否则,若这两个条件都满足,那么我们可通过判定 S 中是否有不动点来判定程序 P 是否终止.

2 实 例

例 2:考虑下列循环的终止性.

$$\begin{aligned}&\textbf{while } x^2+y^2\leqslant 1 \ \&\&\ x\geqslant 0 \ \&\&\ y\geqslant 0 \textbf{ do}\\&\quad x:=2x^2-3xy+1\\&\quad y:=xy+7x+5\\&\textbf{endwhile}\end{aligned}\tag{4}$$

令 $F=(f_1,f_2)=(2x^2-3xy+1,xy+7x+5)^T$,$S=\{X\in R^2:x^2+y^2\leqslant 1,x\geqslant 0,y\geqslant 0\}$为有界闭连通的.调用算法 1,得到 $N^*=3$,则 $I_3=\langle |F(X)|^2-|X|^2,|F^2(X)|^2-|X|^2,|F^3(X)|^2-|X|^2\rangle$.根据算法 2,首先计算 I_3 的 Groebner 基 $G_3=(3y^2-2+24x-17y,xy+5+7x-y,2x^2+16+20x-3y)$,然后根据理想成员判定算法得知:

- $f_1-x=0\cdot(3y^2-2+24x-17y)+(-3)\cdot(xy+5+7x-y)+1\cdot(2x^2+16+20x-3y)$;
- $f_2-y=0\cdot(3y^2-2+24x-17y)+1\cdot(xy+5+7x-y)+0\cdot(2x^2+16+20x-3y)$.

故 $f_1-x\in G_3,f_2-y\in G_3$.根据命题 8 可知 $V_C(I_3)=V_C(I_3(X))=V_C(F(X)-X)$,满足定理 9 的条件(i).为验证条件(ii)是否成立,我们调用 BOTTEMA 得知:当$\hbar=10^{-20}$ 时,有$||F(X)|^2-|X|^2|\geqslant\hbar||F^2(X)|^2-|X|^2|$且$||F(X)|^2-|X|^2|\geqslant\hbar||F^3(X)|^2-|X|^2|$,从而满足定理 9 的条件(ii).因此根据定理 9,由于迭代映射 F 的不动点都不在 S 中,因此该循环是可终止的.

例 3:考虑下列循环的终止性:

$$\begin{aligned}&\textbf{while } x\leqslant 1\ \&\&\ x\geqslant -4\ \&\&\ y\leqslant 2\ \&\&\ y\geqslant -1 \textbf{ do}\\&\quad x:=-7-y-4x^2-y^2\\&\quad y:=-62x+4y+5\\&\textbf{endwhile}\end{aligned}\tag{5}$$

令 $F=(-7-y-4x^2-y^2,-62x+4y+5)^T$,$S=\{X\in R^2:x\leqslant 1,x\geqslant -4,y\leqslant 2,y\geqslant -1\}$为有界闭连通的.调用算法 1,得到 $N^*=3$,则 $I_3=\langle |F(X)|^2-|X|^2,|F^2(X)|^2-|X|^2,|F^3(X)|^2-|X|^2\rangle$.调用算法 2,可判定出 $V_C(I_3)=V_C(F(X)-X)$.同时,调用 BOTTEA 可知,当$\hbar=10^{-4}$ 时,有:

$$||F^3(X)|^2-|X|^2|\geqslant\hbar||F(X)|^2-|X|^2|\text{且}||F^3(X)|^2-|X|^2|\geqslant\hbar||F^2(X)|^2-|X|^2|.$$

故满足定理 9 的两个条件.由于迭代映射 F 的不动点都不在 S 中,根据定理 9,该循环是可终止的.

在表 1 中,我们列举了更多实例来阐明本文方法的适用性.

Table 1 More Examples

表 1 更多实例

实例	定理 9 的条件(i)	定理 9 的条件(ii)	终止性
while ($x\geqslant 1$ && $y\geqslant 1$ && $x\leqslant 3$ && $y\leqslant 3$) do $x:=2x-y^2;y:=3y^2-1$	满足	满足	终止
while ($x^2+y^2\leqslant 3$) do $x:=4x-y;y:=2y+1$	满足	不满足	ND
while ($x\geqslant 1$ && $y\geqslant 1$ && $x\leqslant 3$ && $y\leqslant 3$) do $x:=3x-7;y:=y^2-5x+1$	不满足	满足	ND
while ($x^2\leqslant 5$ && $y\leqslant x$ && $y\geqslant 1$) do $x:=x-7;y:=3x+y$	满足	满足	终止
while ($x^2\leqslant 5$ && $y\leqslant 1$ && $y\geqslant -1$) do $x:=x-y;y:=2x+5y$	满足	满足	不终止
while ($y\geqslant x^2$ && $y\leqslant x$) do $x:=xy-2x+y;y:=-5y+x+x^2-7$	满足	满足	终止
While ($y\leqslant x$ && $x\geqslant 3$ && $x\leqslant 100$) do $x:=3x-y-1;y:=y^2-4x$	满足	满足	终止

表中的 ND 表示本文方法对其终止性无法确定.

3 复杂度

从算法 3 中可以看出:主要的计算都集中在 S2~S5,且涉及的计算主要包括 Grobner 基计算和柱形代数分解.Groebner 基是 Buchberger 在他的博士论文中首先引进的,该方法能从任意多项式理想的一组给定生成元有效地计算出另一组性质良好的生成元,即 Groebner 基.Collins 在 1975 年首次提出了较为实用的基于柱形代数分解

的量词消去算法,用于实闭域上的量词消去问题.S2 中主要计算多项式理想的约化 Groebner 基,在文献[23]中,其计算复杂度在糟糕情形下被证明是 $2^{2^{O(n)}}$,其中,n 为多项式变元个数,该复杂度是双指数的.S3 中涉及理想成员的判定计算,即,判定给定多项式 f 是否属于理想 I,这等价于在给定相同的项序下判定理想 $I\cup\{f\}$ 与理想 I 是否相等.而后者的判定等价于计算两个理想的约化 Groebner 基是否相等(理想的约化 Groebner 基总是唯一的).既然在 S2 中计算理想的约化 Groebner 基的复杂度糟糕情况下是双指数的,因此,S3 的计算复杂度在糟糕情形下也是双指数的.在 S4 和 S5 中,我们采用 Collins 提出的基于柱形代数分解(CAD)的量词消去技术来判定半代数系统是否有实解.而 CAD 的计算复杂度在最糟糕情形下被证明是 $O(2^{2^{(n-2)/5}})$ (n 是变元个数)也是双指数的[24,25].因此,算法 3 的复杂度在糟糕情形下不可避免是双指数的.

4 结 论

借助计算机代数中的 Groebner 基理论,本文研究了一类单重无分支非线性循环程序的终止性问题.尽管程序终止性问题被证明是不可判定的,但对本文所研究的这类循环程序,我们证明了在给定条件下,此类循环的终止性判定问题可归约为不动点的判定问题,而不动点的计算可被规约为半代数系统的求解.本文采用的柱形代数分解(CAD)和 Groebner 基计算都是精确的符号计算,从而导致本文呈现的算法是指数时间复杂度的.尽管高复杂度,但当问题规模不大时,可以在合理时间内得到判定结果.随着近年来符号-数值混合 CAD 技术以及并行 Groebner 基计算的发展,本文算法的效率有望得到提升.我们今后的工作将继续沿此思路探索更加一般的循环程序的终止性,并将其终止性的判定问题归结为不动点的判定问题.

致谢 感谢上海高可信计算重点实验室对作者的支持.

References:

[1] Liu K, Shan ZG, Wang J, He JF, Zhang ZT, Qin YW. Overview on major research plan of trustworthy software. Bulletin of National Natural Science Foundation of China, 2008,22(3):145−151 (in Chinese with English abstract).

[2] Yang L, Xia BC. Mechanical Inequality Proving and Automated Discovering. Beijing: Science Press, 2008 (in Chinese).

[3] Babic D, Cook B, Hu AJ, Rakamaric Z. Proving termination of nonlinear conmmand sequences. Formal Aspects of Computing, 2013,25(3):389−403. [doi: 10.1007/s00165-012-0252-5]

[4] Bagnara R, Mesnard F, Pescetti A, Zaffanella E. A new look at the automatic synthesis of linear ranking functions. Information and Computation, 2012,215:47−67. [doi: 10.1016/j.ic.2012.03.003]

[5] Ben-Amram AM, Genaim S. On the linear ranking problem for integer linear-constraint loops. In: Proc. of the 40th Annual ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. New York: ACM Press, 2013. 51−62. [doi: 10.1145/2429069.2429078]

[6] Bradley A, Manna Z, Sipma H. Termination of polynomial programs. In: Proc. of the 6th Int'l Conf. on Verification, Model Checking, and Abstract Interpretation. Berlin, Heidelberg: Springer-Verlag, 2005. 113−129. [doi: 10.1007/978-3-540-30579-8_8]

[7] Braverman M. Termination of integer linear programs. In: Proc. of the 18th Int'l Conf. on Computer Aided Verification. Berlin, Heidelberg: Springer-Verlag, 2006. 372−385. [doi: 10.1007/11817963_34]

[8] Chen HY, Cook B, Fuhs C, Nimkar K, O'Hearn P. Proving nontermination via safety. In: Proc. of the 20th Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems. Berlin, Heidelberg: Springer-Verlag, 2014. 156−171. [doi: 10.1007/978-3-642-54862-8_11]

[9] Chen YH, Xia BC, Yang L, Zhou C. Discovering non-linear ranking functins by solving semi-algebraic systems. In: Proc. of the 4th Int'l Colloquium on Theoretical Aspects of Computing. Berlin, Heidelberg: Springer-Verlag, 2007. 34−49. [doi: 10.1007/978-3-540-75292-9_3]

[10] Coln M, Sipma HB. Practical Methods for Proving Program Termination. Berlin, Heidelberg: Springer-Verlag, 2002. 227−240. [doi: 10.1007/3-540-45657-0_36]

[11] Coln M, Sipma HB. Synthesis of linear ranking functions. In: Proc. of the 7th Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems. Berlin, Heidelberg: Springer-Verlag, 2001. 67−81. [doi: 10.1007/3-540-45319-9_6]

[12] Cook B, Podelski A, Rybalchenko A. Proving program termination. Communications of the ACM, 2011,54(5):88−98. [doi: 10.1145/1941487.1941509]

[13] Gupta A, Henzinger T, Majumdar R, Rybalchenko A, Xu RG. Proving non-termination. In: Proc. of the 35th Annual ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. New York: ACM Press, 2008. 147−158. [doi: 10.1145/1328438.1328459]

[14] Cousot P. Proving program invariance and termination by parametric abstraction, langrangian relacation and semidefinite programming. In: Proc. of the 6th Int'l Conf. on Verification, Model Checking, and Abstract Interpretation. Berlin, Heidelberg: Springer-Verlag, 2005. 1−24. [doi: 10.1007/978-3-540-30579-8_1]

[15] Podelski A, Rybalchenko A. A complete method for the synthesis of linear ranking functions. In: Proc. of the 5th Int'l Conf. on Verification, Model Checking, and Abstract Interpretation. Berlin, Heidelberg: Springer-Verlag, 2004. 239−251. [doi: 10.1007/978-3-540-24622-0_20]

[16] Tiwari A. Termination of linear programs. In: Proc. of the 16th Int'l Conf. on Computer Aided Verification. Berlin Heidelberg: Springer-Verlag, 2004. 70−82. [doi: 10.1007/978-3-540-27813-9_6]

[17] Xia BC, Yang L, Zhan NJ, Zhang ZH. Symbolic decision procedure for termination of linear programs. Formal Aspects of Computing, 2009,23(2):171−190. [doi: 10.1007/s00165-009-0144-5]

[18] Xia BC, Zhang ZH. Termination of linear programs with nonlinear constraints. Journal of Symbolic Computation, 2010,45(11):1234−1249. [doi: 10.1016/j.jsc.2010.06.006]

[19] Yang L, Zhan NJ, Xia BC, Zhou CC. Program verification by using DISCOVERER. In: Proc. of the Verified Software: Theories, Tools, Experiments. Berlin, Heidelberg: Springer-Verlag, 2008. 528−538. [doi: 10.1007/978-3-540-69149-5_58]

[20] Yang L, Zhou CC, Zhan NJ, Xia BC. Recent advances in program verification through computer algebra. Frontiers of Computer Science in China, 2010,4(1):1−16. [doi: 10.1007/s11704-009-0074-7]

[21] Collins GE. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Proc. of the Automata Theory and Formal Languages. Berlin, Heidelberg: Springer-Verlag, 1975. 134−165. [doi: 10.1007/978-3-7091-9459-1_4]

[22] Cox D, Little J, O'Shea D. Ideas, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry. New York: Springer-Verlag, 1992. [doi: 10.1007/978-0-387-35651-8]

[23] Mayr EW. Some complexity results for polynomial ideals. Journal of Complexity, 1997,13:303−325. [doi: 10.1006/jcom.1997.0447]

[24] Davenport JH, Heintz J. Real quantifier elimination is doubly exponential. Journal of Symbolic Computation, 1988,5:29−35. [doi: 10.1016/S0747-7171(88)80004-X]

[25] Brown CW, Davenport JH. The complexity of quantifier elimination and cylindrical algebraic decomposition. In: Proc. of the ISSAC. New York: ACM Press, 2007. 54−60. [doi: 10.1145/1277548.1277557]

[26] Hidenao I, Hitoshi Y, Hirokazu A. An effective implementation of symbolic-numeric cylindrical algebraic decomposition for optimization problems. In: Proc. of the SNC. New York: ACM Press, 2011. 168−177. [doi: 10.1145/2331684.2331712]

[27] Strzeboński AW. Cylindrical algebraic decomposition using validated numerics. Journal of Symbolic Computation, 2006,41(9):1021−1038. [doi: 10.1016/j.jsc.2006.06.004]

[28] Mityunin VA, Pankratiev EV. Parallel algorithms for Groebner-basis construction. Journal of Mathematical Sciences, 2010,142(4):2249−2266. [doi: 10.1007/s10958-007-0136-z]

附中文参考文献:

[1] 刘克,单志广,王戟,何积丰,张兆田,秦玉文.可信软件基础研究重大研究计划综述.中国科学基金,2008,22(3):145−151. [doi:10.3969/j.issn.1000-8217.2008.03.005]

[2] 杨路,夏壁灿.不等式机器证明与自动发现.北京:科学出版社,2008.

李轶(1980－),男,重庆人,博士,副研究员,主要研究领域为程序验证,符号计算.

冯勇(1965－),男,博士,研究员,博士生导师,主要研究领域为符号数值混合计算.