软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(5):1045−1052 [doi: 10.3724/SP.J.1001.2012.03982]

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

非线性循环的终止性分析*

李 轶+

(电子科技大学 计算机推理与可信计算实验室,四川 成都 610054)

Termination Analysis of Nonlinear Loops

LI Yi+

(Laboratory of Computer Reasoning and Trustworthy Computing, University of Electronic Science and Technology of China, Chengdu 610054, China)

+ Corresponding author: E-mail: zm_liyi@163.com

Li Y. Termination analysis of nonlinear loops. *Journal of Software*, 2012,23(5):1045−1052. http://www.jos.org.cn/1000-9825/3982.htm

Abstract: The termination of linear loops has been studied extensively, but there are few results collected on termination of nonlinear loops. Through the fixed point theorem, this paper presents an approach to the decision of termination of a class of nonlinear loops. In addition, for a particular class of loops, the paper gives a condition under which the termination of the loops is decidable.
Key words: trustworthy computing; nonlinear loop; termination analysis; DISCOVERER

摘 要: 单重线性循环程序的终止性问题已被广泛研究,而有关非线性循环终止性判定的结果甚少.利用不动点理论研究了 n 维单重非线性循环的终止性问题,并建立了相应的符号判定算法.同时,对几类特殊循环的终止性进行了分析,得出了相应的结论.
关键词: 可信计算;非线性循环;终止性分析;DISCOVERER
中图法分类号: TP301 **文献标识码**: A

随着计算机和互联网的迅猛发展,以通信、存储和计算为核心的信息基础设施已经渗透到政治、经济、军事、文化以及社会的各个层面.软件是信息基础设施的灵魂,但它并不总是让人信任,从而产生软件可信性问题.国际上由于软件缺陷而导致的重大灾难、事故和巨大损失屡见不鲜:1986 年,美国的 Therac 25 发射治疗机由于计算机控制程序在某种情况下造成放射线剂量超过正常值几百倍,引起两人死亡;1996 年 6 月 4 日,在欧洲阿丽亚娜 5 型火箭的首次发射中,由于惯性参考系统软件的数据转换错误引起操作失误,致使火箭在发射 40 秒后爆炸,造成 25 亿美元的经济损失;2004 年 12 月 20 日,美国空军第 422 测试评估大队的一架 F22 战斗机因软件问题在起飞过程中失控坠毁.因此,软件可信性问题已经成为国际上一个普遍关注的问题,如何对软件进行自动验证并设计出高可信软件已成为计算机领域一个极具挑战性的问题[1].

一般地,程序验证主要研究 3 个方面的问题:可达性、终止性以及不变量[2].而不包括终止性分析的验证被

* 基金项目: 国家自然科学基金(90718041); 上海市高可信计算重点实验室开放课题(07dz22304200801)
收稿时间: 2010-05-24; 修改时间: 2010-09-29; 定稿时间: 2010-12-15
CNKI 网络优先出版: 2011-05-12 11:47, http://www.cnki.net/kcms/detail/11.2560.TP.20110512.1147.003.html

称为程序的部分正确性证明[3].因此,程序的终止性分析是保证程序完全正确的必要基础.目前,国内外对终止性的研究往往从两个方面进行:一方面,利用 Floyd,Hoare,Dijkstra 等人提出的秩函数(ranking function)法来证明循环的终止[4−6];另一方面,不是通过合成秩函数,而是采用代数理论严格分析并证明循环的终止性[3,7−12].前一种方法是充分而非必要的,即人们很容易构造出没有秩函数但仍可终止的循环程序;后一个方面从可判定角度严格论证某类循环的终止性,因而是完备的.

线性循环程序的终止性问题已被广泛研究[5,7,9,10],但非线性循环程序的终止性分析一直都是十分困难的问题.现有的文献大多采用合成秩函数的方式来证明其终止性,从可判定角度来分析其终止性的研究成果相当少.文献[11]通过分析多项式映射 f 的发散区间$(-\infty,fix_{\min})$,$(fix_{\max},+\infty)$讨论了一类多项式循环的终止性问题.$fix_{\min}$,$fix_{\max}$分别为 f 的最小、最大不动点.文献[13]针对含单个变元(一维)且迭代仅在 1 个区间上进行的循环建立了终止性判定方法.文献[8]分析了循环条件为非线性多项式约束,而赋值语句为线性的循环的终止性.在本文中,我们证明了在给定合适的条件下,不动点理论可以建立 n 维单重非线性循环的终止性判定算法.

1 主要结果

在这节,我们将给出一个条件,使得对一般的无初始条件的单重循环程序,当其满足该条件时终止性是可判定的,并给出了符号判定算法.此外,对几类特殊的循环程序,我们也给出了相应的条件,使得当循环满足各自的条件时,终止性也是可判定的.特别是对一类迭代映射为 $A\in\mathbb{R}^{2\times 2}$ 的循环程序,给出了独立于不动点理论的判定方法.

1.1 一般形式的非线性循环

这一节中,我们对具有一般形式的非线性循环,即赋值语句和(或)循环条件为非线性表达式的程序进行了研究,并给出了一个条件,使得满足此条件时,其终止性是可判定的.我们首先陈述下列简单定理,它是本节算法的基石.

定理 1. 设 S 是 n 维空间中的一个闭集.给定 n 维连续映射 $F:X\mapsto F(X)$.若对任意的 $X\in S$ 满足条件:

$$\|F(X)-F^2(X)\|\leqslant L\|X-F(X)\|,\ L<1,$$

则下面的循环程序

$$\left.\begin{array}{l}\text{while } X \text{ in } S \text{ do}\\ \qquad \{X=F(X)\}\\ \text{endwhile}\end{array}\right\}\tag{1}$$

存在输入 $X\in\mathbb{R}^n$,使得程序不终止的充分必要条件是 $F(X)$在 S 上有不动点.

证明:这个证明很简单.

(必要性的证明):若循环(1)是不可终止的,则必存在无穷迭代:

$$Seq=\{X_0,X_1,X_2,\dots,X_n,\dots\}=\{F^n(X_0)\}_{n=0}^{\infty}\subseteq S.$$

对 $m>n$,有

$$\begin{aligned}\|X_m-X_n\|&\leqslant\|X_m-X_{m-1}\|+\|X_{m-1}-X_{m-2}\|+\dots+\|X_{n+1}-X_n\|\\&\leqslant\sum_{i=n}^{m-1}L^i\|F(X_0)-X_0\|\\&=(L^n+\dots+L^{m-1})\|F(X_0)-X_0\|\\&=L^n\frac{1-L^{m-n}}{1-L}\|F(X_0)-X_0\|.\end{aligned}$$

由 $0<L<1$,得到:

$$\|X_m-X_n\|\leqslant\frac{L^n}{1-L}\|F(X_0)-X_0\|.$$

因此,当 $n\to\infty,m\to\infty$ 时,$\|X_m-X_n\|\to 0$.即 $Seq=\{X_n\}_{n=1}^{\infty}$ 是柯西收敛序列.故存在 $\bar{X}$,$\lim_{n\to\infty}X_n=\bar{X}$.由连续性可知,

$$\bar{X}=\lim_{n\to\infty}X_n=F(\lim_{n\to\infty}X_{n-1})=F(\bar{X}).$$

(充分性的证明):若 $F(X)$在 S 上有不动点 $\bar{X}$,则对任意的 n=1,2,…, $F^n(\bar{X})=\bar{X}\in S$.这表明循环在 $\bar{X}$ 处不可终止.证毕. □

上述定理中的映射 F 并未要求是自映射.此外,定理 1 中的条件可以减弱.因此,令 $G=F^k$,可得下面的推论：

推论 1. 记号同上.若存在 $k\in\mathbb{N}$,使得对任意的 $X\in S$,有 $F^i(X)\in S$,i=1,2,…,k−1,且满足:

$$\|F^k(X)-F^{2k}(X)\|\leqslant L\|X-F^k(X)\|,\ L<1,$$

则程序(1)不终止的充分必要条件是 $F(X)$在 S 上存在长度为 k 的周期轨.

证明:充分性是显然的,下面主要证明必要性.假设满足题设的 k 存在,则令 $G=F^k$.显然,G 满足定理 1 的题设条件.故根据定理 1 可知,$\exists\bar{X}\in S$,使得 $G(\bar{X})=\bar{X}$.又因为对任意的 $i=1,2,...,k-1$,$F^i(\bar{X})\in S$,因此 $F(X)$在 S 上存在长度为 k 的周期轨.证毕. □

根据定理 1,我们首先要判定循环是否满足定理 1 的题设,即判定下列优化问题的最大值 L<1:

$$\left.\begin{aligned}&L=\max\frac{\|F(X)-F^2(X)\|}{\|X-F(X)\|}<1\\&\text{s.t. }X\in S\end{aligned}\right\}\qquad(2)$$

在判定上述优化问题时,我们将借助符号计算工具 BOTTEMA,其主要功能在于几何代数不等式的批量验证、优化问题的求解等等[14−16].利用 BOTTEMA,我们能得到包含上述优化问题最优值 L 的长度任意小的区间,从而可判定 L 是否小于 1.整个过程均是符号的(即纯符号变量之间的四则运算以及有理数域上的精确计算),并不会涉及到任何近似计算.当循环满足公式(2)时,则计算其映射的不动点,并将其代入循环条件中检验.这一步骤可等价于半代数系统的求解问题,即判定下列半代数系统 SAS 是否有解:

$$\{X\mid F(X)-X\}\cap S.$$

因此,我们也将采用符号计算工具DISCOVERER来处理,其主要功能包括半代数系统的实解分类以及实根隔离等[15,17,18].综上所述,上述两个判定过程均是符号的,不会涉及近似计算.因此对一般的非线性循环,根据定理 1,我们给出了相应的判定算法.

算法.

输入:非线性循环程序的迭代映射 F,循环条件形成的区域 S.

输出:T(终止),NT(不可终止),ND(不能确定).

S1. 若 $S=\varnothing$,返回 T;

S2. 若 $S\neq\varnothing$,则,

  S2.1. 通过 BOTTEMA 判定映射 F 是否满足条件(2);若不满足则返回 ND,反之则转 S2.2;

  S2.2. 通过 DISCOVERER 判定半代数系统 SAS 是否有解.若有则返回 NT,否则返回 T.

例 1:考虑循环(3)的终止性.

$$\left.\begin{aligned}&\text{while } x^2+y^2<1\wedge x>0\wedge y>0 \text{ do}\\&\quad x:=\frac{x^2}{3}-y-1\\&\quad y:=\frac{y}{10}+\frac{1}{7}\\&\text{endwhile}\end{aligned}\right\}\qquad(3)$$

根据上述算法,需要验证循环(3)中的映射是否满足条件(2).通过调用 BOTTEMA 得到 $L\in\left(\frac{38}{39},1\right)$,因此满足定理题设.然后判定映射的不动点是否落在循环条件构成的区域中,这等价于判定下面的半代数系统 SAS 是否有解:

$$SAS:\left\{\frac{x^2}{3}-y-1-x=0,\frac{y}{10}+\frac{1}{7}-y=0,x^2+y^2<1,x>0,y>0\right\}.$$

调用 DISCOVERER 中的函数 *realzeros*[**]

$$realzeros\left(\left[\frac{x^2}{3}-y-1-x,\frac{y}{10}+\frac{1}{7}-y\right],[\ ],[1-x^2-y^2,x,y],[\ ],[x,y],1/100\right).$$

其返回"The number of solutions is 0".这表明映射的不动点不在循环条件围成的区域内,故该循环是可终止的.整个判定过程是全符号的,并不会涉及近似计算.

令 $F(X)=(f_1(X),f_2(X),...,f_n(X))^T,X=(x_1,x_2,...,x_n)^T,\mu_{ij}(X)=\frac{\partial f_i(X)}{\partial x_j}$,下面的命题给出了使迭代映射 F 满足 Lipschitz 条件的充分条件.

命题 1. 记号同上.给定循环程序(1)且 S 为闭凸集.如果对任意的 $i,j,X\in S,\exists L<\frac{1}{n+\varepsilon}(\varepsilon>0)$,使得

$$|\mu_{ij}(X)|\leqslant L,$$

则循环(1)是不可终止的充分必要条件是 $F(X)$在 S 中存在不动点.

证明:任给 $X,Y\in S$.根据多元微分中值定理,有

$$|f_i(Y)-f_i(X)|^2=\left|\sum_{j=1}^n\frac{\partial f_i}{\partial x_j}(\xi)(y_j-x_j)\right|^2\leqslant\left(\sum_{j=1}^n\left|\frac{\partial f_i}{\partial x_j}(\xi)\right|\cdot|(y_j-x_j)|\right)^2\leqslant L^2\cdot\left(\sum_{j=1}^n|y_j-x_j|\right)^2\leqslant nL^2\cdot\sum_{j=1}^n|y_j-x_j|^2.$$

$\xi=X+\theta(Y-X)\in S,\theta\in(0,1),i=1,\dots,n$.由$\|\cdot\|$的定义易知,$\|F(X)-F(Y)\|^2\leqslant n^2L^2\|X-Y\|^2$.令 $L'^2=n^2L^2$.又因为 $L<\frac{1}{n+\varepsilon}$,因此$\exists L',0<L'<1$,有$\|F(X)-F(Y)\|\leqslant L'\|X-Y\|$.故 F 在 S 上满足 Lipschitz 条件.类似于定理 1 的证明,根据三点不等式可得结论成立.证毕. □

1.2 特殊形式的非线性循环

这一节中,我们将考虑循环(1)的迭代映射 F 的几种特殊的形式,并建立相应的结果.

命题 2. 记号同上.假设在循环程序(1)中的赋值语句为 $X:=AX,A\in\mathbb{R}^{n\times n}$.如果 A 的所有特征值$|\xi_i|<1$,则循环(1)不可终止的充分必要条件是原点 $O\in S$.

证明:由矩阵分析中的一个结论:当 $n\to\infty$时,矩阵 $A^n\to 0$,当且仅当 A 的所有特征值的模小于 1.因此,若该循环程序不可终止,由 $X_n=A^nX_0$ 可知,序列 $\{X_n\}_{n=0}^{\infty}$ 收敛到原点 $O\in S$.证毕. □

命题 3. 记号同上.给定循环程序(1).假设在赋值语句中至少$\exists i$,有 $x_i=f_i(x_i)$.记 $X^0=(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n)^T,F^0=[f_1,\dots,f_{i-1},f_{i+1},\dots,f_n]^T$ 为$\mathbb{R}^{n-1}\mapsto\mathbb{R}^{n-1}$ 的 $n-1$ 维映射.记$\pi_1:\mathbb{R}^n\mapsto\mathbb{R}^{n-1}$. $u^0=(u_1^*,...,u_{i-1}^*,u_{i+1}^*,...,u_n^*)$ 为 F^0 在$\pi_1(S)$上的不动点.l_0 为过 u^0 点且与 x_i 轴平行的直线,且 $\overline{l}^0=l_0\cap S$.当满足如下条件时,循环(1)不终止的充分必要条件是 F 在 S 中有不动点:

(1) $\forall X^0\in\pi_1(S)$,定理 1 的条件成立;

(2) $\overline{l}^0$ 仅为一个区间.

证明:若循环不终止,则存在 $Seq=\{X_0,X_1,\dots,X_n,\dots\}$.由条件(1)可知,每个 X_i 的其余 $n-1$ 个分量形成的点列必收敛到$\pi_1(S)$上的不动点 u^0.因此,Seq 逼近 $\overline{l}^0$.那么,既然在平行于 x_i 轴的区间 $\overline{l}^0$ 上存在关于第 i 个分量的无穷迭代 $\{x_j^i\}_{j=0}^{\infty}$,这里,x_j^i 表示 X_j 的第 i 个分量,根据文献[13]中的定理 1 可知,必在 $\overline{l}^0$ 上有不动点 x_i^*.因此,F 在 S 上存在不动点 $(u_1^*,...,u_i^*,...,u_n^*)$.证毕. □

文献[8]中研究了一类特殊的非线性循环的终止性.

** 若半代数系统有实解,则 *realzeors* 能将各个解隔离,即返回一系列立方体,使得其每个立方体中仅包含 1 个实解.

$$\left.\begin{array}{l}\text{while } X \in S_{poly} \text{ do} \\ \quad \{X := AX\}\ (A \in \mathbb{R}^{n\times n}) \\ \text{endwhile}\end{array}\right\} \tag{4}$$

其中,$S_{poly}=\{X|p_1(X)>0,p_2(X)>0,\dots,p_k(X)>0,p_i\in\mathbb{K}[X]\}$.文献[8]证明,在满足适定条件下,循环(4)的终止性是可判定的.针对循环(4),本节余下的部分将着重分析 $A\in\mathbb{R}^{2\times 2}$ 的情形.不同于之前建立的结果,下面的结论将不依赖于不动点理论,也并不同于文献[8]中的方法.令 $X=(x_1,\dots,x_n)$, $p_d(X)=\left\{p(X)\in\mathbb{K}[X]\,|\,p(X)=\sum_{|\alpha|=d}c_\alpha X^\alpha\right\}$.其中,$\alpha=(\alpha_1,\alpha_2,\dots,\alpha_n), |\alpha|=\sum_{i=1}^{n}\alpha_i$.考虑带赋值矩阵 $A\in\mathbb{R}^{n\times n}$ 的循环 P_1.

$$\begin{array}{ll} P_1:\ \text{while } T(X)>0 \text{ do} & P_2:\ \text{while } T(CU)>0 \text{ do} \\ \qquad \{X:=AX\} & \qquad \{U:=C^{-1}ACU\} \\ \quad \text{endwhile} & \quad \text{endwhile}\end{array}$$

其中,$T(X)\in\mathbb{K}[X]$,$C^{-1}AC=diag(J_1,J_2,\dots,J_k)$为 A 的 Jordan 标准型.

命题 4. 记号同上.程序 P_1 是不可终止的,等价于程序 P_2 是不可终止的.

证明:若 P_1 在点 X^*处不可终止,则 P_2 在点 $U^*=C^{-1}X^*$处不可终止;反之,若 P_2 在点 U^*处不可终止,则 P_1 在点 CU^*处不终止.证毕. □

下面,我们将限制 P_1 程序中的赋值矩阵 $A\in\mathbb{R}^{2\times 2}$.既然 P_1 的终止性等价于 P_2 的终止性,则需要分析 A 的 Jordan 标准型.有 3 种情形:

$$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix},\ \begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix},\ \rho\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}.$$

ρ为复特征值的模.在前两种情况下,既然 A 仅有实特征值,那么终止性分析是非常简单的.故我们主要分析第 3 种情形,即 A 有复共轭特征值.特别地,既然当 $\frac{\theta}{\pi}\in Q$ (有理数域)时其轨道是周期的,从而也非常容易判定其终止性.因此,这里我们仅考虑 $\frac{\theta}{\pi}\notin Q$ 的情形.同时,我们进一步限制 P_1 程序中 $T(X)\in p_d(X)$为齐 d 次的多项式.因此,程序 P_2 中的 $T(CU)\in p_d(U)$.故有下列命题成立:

命题 5. 记号同上.假设程序 P_1,P_2 中的赋值矩阵 $A\in\mathbb{R}^{2\times 2}$,且仅有复特征值,则程序 P_2 不可终止等价于程序 P_3 是不可终止的.

$$\begin{array}{l} P_3:\ \text{while } T(CU)>0 \text{ do} \\ \quad U:=\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}U,\ \frac{\theta}{\pi}\notin Q \\ \text{endwhile}\end{array}$$

证明:为方便起见,分别令 B_1,B_2 为程序 P_2,P_3 各自的赋值矩阵,则有 $T(CB_1^nU)=\rho^{nd}T(CB_2^nU),\rho>0$.因此,$P_1,P_2$ 有相同的不可终止点集.证毕. □

在程序 P_3 中,线性映射 $B_2=\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$是一个旋转映射.因为 $\frac{\theta}{\pi}\notin Q$,由此,$\mathbb{R}^2$ 上任一非零点 U 在圆周 $r=||U||_2$ 上的迭代轨道是稠密的.倘若在区域$\{U|T(CU)>0\}$中存在圆周 $r=||U||_2$,则程序 P_3 是不可终止,反之则必然终止.这等价于判定下面的量词消去问题:

$$\exists r\forall u_1\forall u_2(u_1^2+u_2^2=r^2\Rightarrow T(CU)>0),U=(u_1,u_2)^T \tag{5}$$

事实上,在大多数情况下,我们只需通过区域$\{U|T(CU)>0\}$的图像就能判定程序 P_3 的终止性,而无须处理上面的量词公式(5).这是因为曲线 $T(CU)$大多不是封闭的,且必以原点 O 为边界点.

例 2:考虑以下程序(6):

$$\left.\begin{array}{l}\text{while } u_1^2-u_2^2>0 \text{ do}\\ \quad \{U:=B_2U\}\\ \text{endwhile}\end{array}\right\} \tag{6}$$

不难看出,循环测试区域为两条直线$y=\pm x$在原点相交形成的两个对角区域.既然对任意的点$U\neq 0$,其迭代轨道是稠密的,则必然在有限步后跳出循环测试区域,因此程序(6)必然终止.因此,当 $T(CU)$不是封闭曲线时,则程序 P_3 总是终止的.对循环程序 P_3,若循环条件中的 $T(CU)=T'(U)$不是齐次的,则可重写成几个齐次多项式之和,$T'(U)=T_k'(U)+...+T_1'(U)+T_0'(U)$.其中,$T_i'(U)\in p_i(U)$.这里,将假设常数$T_0'(U)<0$.将程序P_3中的$T(CU)$分别替换为$T'(U),T_k'(U),...,T_0'(U)$,得到程序$P_3',P_{3_k}',...,P_{3_0}'$.对 $i=1,2,\ldots,k$,记 S_i 为区域$\{U\mid T_i'(U)>0\}$,$\overline{S_i}$ 为它的补.

命题 6. 记号如上.假设$T'(U),T_k'(U),...,T_1'(U)$均不是封闭曲线,$T_0'(U)<0$,$S_i\neq\mathbb{R}^2\setminus\{0\}$,$i=1,\ldots,k$.若$\bigcup_{i=1}^{k}S_i\neq\mathbb{R}^2\setminus\{0\}$,则程序$P_3'$必终止.

证明:因为当$T_k'(U),...,T_1'(U)$均不是封闭曲线时,则S_i均为无界区域.

因此由上述讨论可知,每个循环$P_{3_k}',...,P_{3_1}'$都必然终止.又因为$T_0'(U)<0$,因此P_{3_0}'也终止.

而当这些程序的循环区域的并集不为$\mathbb{R}^2\setminus\{0\}$时,则必存在$N$,使得对每个程序$P_{3_i}'$,在迭代到$N$次时,各自的迭代点都可落入到$\overline{\bigcup_{i=1}^{k}S_i}$,同时可终止,从而使得循环$P_3'$终止.证毕. □

例 3:考虑以下程序(7):

$$\left.\begin{array}{l}\text{while } u_1^2-u_2^2+u_2-3>0 \text{ do}\\ \quad \{U:=B_2U\}\\ \text{endwhile}\end{array}\right\} \tag{7}$$

根据命题 5 可知该循环必然终止,但文献[8]的算法不能处理.文献[8]中的方法首先会将B_2^nU带入到循环条件得到新的条件表达式 $Cond(U,\sin(2n\pi\alpha),\cos(2n\pi\alpha),\sin(2n\pi\alpha 2\alpha),\cos(2n\pi\alpha 2\alpha))>0$.然后判定表达式中$\alpha,2\alpha$是否有理无关:若是,则可分别用 $x_i,y_i(i=1,2)$来代替里面的几个三角函数,并加上约束$x_i^2+y_i^2=1$;若有理相关,则文献[8]中的算法不能进行判定.$\alpha,2\alpha$有理无关等价于$\alpha,2\alpha,1$ 在 Q 上线性无关.对循环(7),由于存在 $k_1=-2,k_2=1,k_3=0$,使得$k_1\alpha+k_2 2\alpha+k_3 1=0$,因此$\alpha,2\alpha$有理相关.

2 更多实例

本节将利用上一节所建立的结论来判定几个循环程序的终止性.由于要么其中的循环条件为根式不等式,要么迭代映射为非线性的,因此文献[8]中的方法均不能处理.

例 4:考虑循环(8)的终止性.

$$\left.\begin{array}{l}\text{while } x^2+y^2\leqslant\dfrac{1}{2}\text{ do}\\ \quad x:=-\dfrac{3}{7}x-\dfrac{1}{5}y^2x-11\\ \quad y:=\dfrac{\sqrt{x^2+y^2}}{4}+3\\ \text{endwhile}\end{array}\right\} \tag{8}$$

通过 BOTTEMA,不难验证它满足命题 1 的题设.

因此,计算其不动点为$X^*=(x^*,y^*)=(-2.230086508,4.185673571)\notin S$,故该循环可终止.

例 5:考虑循环(9)的终止性.

$$\left.\begin{array}{l}\textbf{while } 2\leqslant\sqrt[5]{x^2+y^2+z^2}\leqslant 7\textbf{ do}\\ \begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}\frac{-3}{16} & -1 & \frac{1}{21}\\ \frac{1}{9} & \frac{-2}{37} & 4\\ \frac{-4}{27} & \frac{1}{11} & \frac{1}{6}\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}\\ \textbf{endwhile}\end{array}\right\} \tag{9}$$

既然赋值矩阵的特征值的模均小于 1,根据命题 2 可知,检验原点 $O\notin S$,故循环可终止.

例 6:考虑循环(10)的终止性.

$$\begin{array}{l}\textbf{while } xy\geqslant 3\wedge y\geqslant\sqrt[3]{x}\wedge yz-\sqrt{xy}\geqslant 0\wedge 3x+4y\leqslant 1\textbf{ do}\\ \left\{x:=\sqrt{\frac{x}{y}}-1, y:=\frac{x}{7y^2}+3, z:=\frac{\sqrt[7]{11z^9-23z^6+8z^3-4z-1}}{z^2+1}\right\}\\ \textbf{endwhile}\end{array} \tag{10}$$

令 $F^0=(f_1(x,y),f_2(x,y))^T$.这里, $f_1=\sqrt{\frac{x}{y}}-1, f_2=\frac{x}{7y^2}+3$.使用命题 1 的方法易知,$F^0$ 在测试区域$\pi_1(S)$上满足 Lipschitz 条件,因此,F^0 在$\pi_1(S)$上有不动点 $u^0=(x_0,y_0)$.过 u^0 作平行于 z 轴的直线:l^0:$x=x_0,y=y_0,z=z_0+t,(t\in\mathbb{R}_\infty)$.令 $\overline{l}^0=S\cap l^0$.将 $x=x_0,y=y_0$ 和 $z=z_0+t,(t\in\mathbb{R}_\infty)$代入到$\{xy\geqslant 3\wedge y\geqslant\sqrt[3]{x}\wedge yz-\sqrt{xy}\geqslant 0\wedge 3x+4y\leqslant 1\}$,不难看出,$t$ 的取值范围为一个区间,因此$\overline{l}^0$ 为一个区间.故循环(10)满足命题 3 的题设.根据命题 3,计算其不动点为

$$\begin{aligned}X^*=\{&(-0.03988851619,-0.04327175931,-0.3961037320)^T,\\&(-0.03988851619,-0.04327175931,-0.3264659532)^T,\\&(-0.03988851619,-0.04327175931,-0.8437019345)^T\}.\end{aligned}$$

经检验,$X^*\notin S$.故根据命题 3 可知,循环可终止.

上述例 4、例 6 的终止性判定完全可采用第 1.1 节提出的符号算法来判定.这是因为虽然它们含有根式,但总能通过引进新变元来代替所出现的根式,从而变成无根式的情形.为行文简洁,这里我们直接使用近似计算来得到不动点.

3 结 论

本文研究了 n 维单重循环程序的终止性.在给定条件下,结合不动点理论,我们给出了此类循环终止性分析的符号判定算法.同时,对迭代映射为 $A\in\mathbb{R}^{2\times 2}$ 的特殊一类循环,给出了独立于不动点理论的方法,并建立了相关的结果.我们将在未来的工作中进一步研究这种方法,使其能够解决更广泛一类的循环终止性问题.

致谢 感谢华东师范大学杨路教授、四川大学张伟年教授给予本文研究工作的建设性意见,感谢上海高可信计算重点实验室对本文研究工作的支持.

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] Rodríguez-Carbonell E, Kapur D. Generating all polynomial invariants in simple loops. Journal of Symbolic Computation, 2007, 42(4):443−476. [doi: 10.1016/j.jsc.2007.01.002]

[3] 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]

[4] Cousot P. Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming. In: Cousot R, ed. Proc. of the VMCAI 2005. LNCS 3385, Heidelberg: Springer-Verlag, 2005. 1−24. [doi: 10.1007/978-3-540-30579-8_1]

[5] Colon M, Sipma HB. Practical methods for proving program termination. In: Proc. of the CAV 2002. Heidelberg: Springer-Verlag, 2002. 442−454. [doi: 10.1007/3-540-45657-0_36]

[6] Chen YH, Xia BC, Yang L, Zhan NJ, Zhou CC. Discovering non-linear ranking functions by solving semi-algebraic systems. In: Jones CB, Liu Z, Woodcock J, eds. Proc. of the ICTAC 2007. LNCS 4711, Heidelberg: Springer-Verlag, 2007. 34−49. [doi: 10.1007/978-3-540-75292-9_3]

[7] 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]

[8] 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]

[9] Tiwari A. Termination of linear programs. In: Alur R, Peled DA, eds. Proc. of the CAV 2004. LNCS 3114, Heidelberg: Springer-Verlag, 2004. 70−82. [doi: 10.1007/978-3-540-27813-9_6]

[10] Braverman M. Termination of integer linear programs. In: Ball T, Jones RB, eds. Proc. of the CAV 2006. LNCS 4144, Heidelberg: Springer-Verlag, 2006. 372−385. [doi: 10.1007/11817963_34]

[11] Babic D, Hu AJ, Rakamaric Z, Cook B. Proving termination by divergence. In: Proc. of the 5th IEEE Int’l Conf. on Software Engineering and Formal Methods. IEEE Press, 2007. 93−102. [doi: 10.1109/SEFM.2007.32]

[12] Li Y. Algebraic approaches to decision of program termination [Ph.D Thesis]. Beijing: Graduate University, the Chinese Academy of Sciences, 2009 (in Chinese with English abstract).

[13] Yao Y. Termination decision of nonlinear programs over intervals. Journal of Software, 2010,21(12):3116−3123 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3722.htm [doi: 10.3724/SP.J.1001.2010.03722]

[14] Yang L. Recent advances in automated theorem proving on inequalities. Journal of Computer Science and Technology, 1999,14(5):434−446. [doi: 10.1007/BF02948785]

[15] Yang L, Xia SH. Automated proving for a class of constructive geometric inequalities. Chinese Journal of Computers, 2003,26(7):769−778 (in Chinese with English abstract).

[16] Yang L, Xia BC. Mechanical Inequality Proving and Automated Discovering. Beijing: Science Press, 2007 (in Chinese).

[17] Yang L, Zhan NJ, Xia BC, Zhou CC. Program verification by using DISCOVERER. In: Meyer B, Woodcock J, eds. Verified Software. LNCS 4171, 2008. 528−538. [doi: 10.1007/978-3-540-69149-5_58]

[18] Yang L, Hou XR, Zeng ZB. A complete discrimination system for polynomials. Science in China (Series E), 1996,39(6):628−646.

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.

[12] 李轶.程序终止性判定的代数算法研究[博士学位论文].北京:中国科学院研究生院,2009.

[13] 姚勇.区间上非线性程序的终止性判定.软件学报,2010,21(12):3116−3123. http://www.jos.org.cn/1000-9825/3722.htm [doi: 10.3724/SP.J.1001.2010.03722]

[15] 杨路,夏时洪.一类构造性几何不等式的机器证明.计算机学报,2003,26(7):769−778.

[16] 杨路,夏壁灿.不等式机器证明与自动发现.北京:科学出版社,2007.

李轶(1980－),男,重庆人,博士,讲师,CCF 会员,主要研究领域为程序验证,计算机自动推理.