软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(6):1133−1142 [doi: 10.13328/j.cnki.jos.004427]

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

有界闭域上的线性赋值循环终止性分析*

李 轶, 吴文渊, 冯 勇

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

通讯作者: 李轶, E-mail: zm_liyi@163.com

摘 要: 对有界闭域上的线性赋值循环程序终止性问题进行研究.利用 Jordan 标准型技术将原循环程序的终止性问题约减为终止性等价的具有简单结构的循环程序的终止性问题.证明了当线性迭代映射满足一定条件时,该类循环程序不可终止的充分必要条件是:迭代映射在有界闭域上有不动点或周期轨.

关键词: 可信计算;非线性循环;终止性分析;Jordan 标准型;有界闭域

中图法分类号: TP301

中文引用格式: 李轶,吴文渊,冯勇.有界闭域上的线性赋值循环终止性分析.软件学报,2014,25(6):1133−1142. http://www.jos.org.cn/1000-9825/4427.htm

英文引用格式: Li Y, Wu WY, Feng Y. Termination analysis of loops with linear assignment over closed and bounded domains. Ruan Jian Xue Bao/Journal of Software, 2014,25(6):1133−1142 (in Chinese). http://www.jos.org.cn/1000-9825/4427.htm

Termination Analysis of Loops with Linear Assignment over Closed and Bounded Domains

LI Yi, WU Wen-Yuan, 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)

Corresponding author: LI Yi, E-mail: zm_liyi@163.com

Abstract: Termination of linear programs over closed and bounded domains is analyzed in this paper. The termination of this class of loops can be reduced to that of another class of loops by means of Jordan canonical forms. It has been shown that under some condition, this kind of loops do not terminate over the domains if and only if there exist fixed points or periodic orbits in the domains.

Key words: trusted computing; non-linear loop; termination analysi; Jordan canonical form; closed and bounded domain

软件可信性问题已经成为国际上一个普遍关注的问题[1].正确性是程序的最重要的属性之一,但不包括终止性分析的验证被称为程序的部分正确性证明[2].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.当前,国际上进行终止性研究的主流方法是寻找循环程序的秩函数(ranking function).如:Colon 和 Sipma[3]借助多面体代数理论去寻找线性程序的线性秩函数;Podelski 和 Rybalchenko[4]首次完备地合成了一类无初始条件的线性程序的线性秩函数,即,如果这类程序有线性秩函数,则通过他们的方法一定可以构造出来.此外,Bradley 及其合作者[5]利用 Farkas 引理去合成线性秩函数.在文献[6]中,Cousot 运用半正定规划工具 SDP 找到了非线性程序的非线性秩函数.但由于 SDP 内部采用数值计算,从而导致结果有可能存在误差.同时,该方法也不能回答所判定的循环程序是否具有预定定形式的秩函数问题.借助柱形代数分解和多项式判别系统等实代数理论,杨路、夏壁灿等人[7,8]利用实代数工具 DISCOVERER 成功找到了非线性循环程序的非线性秩函数,扩大了可自动验证程序的范围.重要的是,他们的方法是精确无误差的,且能够回答给定循环是否具有预定形式的秩函数问题.但是,秩函数的存在仅仅是循环程序可终止的充分而非必要条件,即能很容易地构造出没有秩函数但仍可终

* 基金项目: 国家自然科学基金(61103110); 重庆市科技攻关项目(cstc2012ggB40004)
收稿时间: 2012-09-03; 修改时间: 2013-02-04; 定稿时间: 2013-05-07

止的循环程序.相比较于循环终止性的秩函数法,文献[9]提出搜索循环可终止的反例.在 2004 年,Tiwari[10]首次从可判定角度证明了一类无初始条件无分支单重线性循环的终止性是可判定的.同时,文献[10]也证明了一般的多分支线性循环程序的终止性问题是不可判定的.2006 年,Braverman 在文献[11]中将 Tiwari 的工作推广到整数环上,并证明了这类循环在整数环上的终止性仍是可判定的.此外,文献[12−14]也证明了这类不带初始条件单重无分支的线性循环的终止性是可判定的.既然一般形式的线性程序终止性是不可判定的,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变得更加困难.这里,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.2007 年,文献[15]通过分析多项式映射 f 的发散区间$(-\infty,fix_{\min})$,$(fix_{\min},+\infty)$讨论了一类多项式循环的终止性问题,$fix_{\max}$,$fix_{\min}$ 分别为 f 的最大、最小不动点.2009 年,文献[16]针对含单个变元(一维)且迭代仅在一个区间上进行的循环建立了终止性判定方法.2010 年,文献[17]首次分析了赋值为线性、循环条件为多项式约束一类非线性循环的终止性,并证明这类循环在满足一定条件下的终止性是可判定的.

本文对赋值为线性、循环条件形成有界闭域的一类非线性循环的终止性问题进行了分析.我们证明了:当赋值矩阵 A 的特征值满足一定条件时,这类循环是不可终止的充分必要条件为映射 A 在循环条件形成的有界闭域上有不动点或周期轨.与文献[17]中分析的程序类型不同,本文的程序类型中,循环条件可以是多项式表达式,也可以是非多项式表达式,且判定方法更加简洁.

1 主要结果

给定矩阵 $A\in R^{n\times n}$,其对应的实 Jordan 标准型记为 $J=diag(J_1(\lambda_1),J_2(\lambda_2),\ldots,J_m(\lambda_m))$.其中,$J_i(\lambda_i)$表示对应于特征值为$\lambda_i$ 的 Jordan 块.$J_i(\lambda_i)$的表达式为下列两者之一:

$$\begin{pmatrix} \lambda_i & 1 & 0 & \ldots & 0 \\ 0 & \lambda_i & 1 & \ldots & 0 \\ 0 & 0 & \lambda_i & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & \lambda_i \end{pmatrix}, \begin{pmatrix} D_i & I & 0 & \ldots & 0 \\ 0 & D_i & I & \ldots & 0 \\ 0 & 0 & D_i & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & I \\ 0 & 0 & 0 & \ldots & D_i \end{pmatrix} \tag{1}$$

这里,$\lambda_i\in R$ 是一个实数;而 D_i 是一个 2×2 的实矩阵,即:

$$D_i=\begin{pmatrix} \alpha_i & -\beta_i \\ \beta_i & \alpha_i \end{pmatrix}=\rho_i\begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}=\rho_i\cdot M_i.$$

显然,在公式(1)中:第 1 种类型的 Jordan 块对应实特征值;而第 2 种类型的 Jordan 块对应复特征值$\alpha_i+i\beta_i$,且有 $|D_i|^2=|\alpha_i+i\beta_i|^2=\rho_i^2$.记号|□|中:□若为复数,则该记号表示复数的模;若为矩阵,则该记号表示矩阵的行列式.

1.1 线性映射A在有界闭域上的迭代终止性分析

我们考虑下列循环程序(2)的终止性问题:

$$\left.\begin{array}{l} \textbf{while } X\in S \textbf{ do} \\ \quad \{X=AX\} \\ \textbf{endwhile} \end{array}\right\} \tag{2}$$

其中,S 是 R^n 中的有界闭集,$A\in R^{n\times n}$,$X\in R^n$;$X=AX$ 表示同时对 X 进行赋值.这里,S 被设定为有界闭的,一方面是因为现实世界中的物理量均是有界的,如速度、加速度等;另一方面是因为 S 的有界闭性质保证了 S 中任意收敛序列的极限都落在 S 中.

定义 1. 循环程序(2)是不可终止的,如果存在点 $X\in S$,使得对任意的非负整数 k,都有 $A^kX\in S$;如果 S 中没有这样的点,则称循环程序(2)是可终止的.

根据下面的结果,可将循环程序(2)的终止性问题等价地转换为另一个程序的终止性问题.新的循环程序其结构更加简单,使得我们更容易分析它的终止性.

定理 2. 记号同上.给定可逆矩阵 $P\in R^{n\times n}$.循环程序(2)在 S 上不可终止,当且仅当循环程序(3):

$$\left.\begin{array}{c}\textbf{while } Y\in \boldsymbol{P}(S) \textbf{ do}\\ \{Y=JY\}\\ \textbf{endwhile}\end{array}\right\} \tag{3}$$

在 $\boldsymbol{P}(S)$上是不可终止的.这里,$\boldsymbol{P}(S)=\{Y\in R^{n\times n}: Y=PX$,对 $X\in S\}$,$J=PAP^{-1}$ 为 A 的实 Jordan 标准型.

证明:若循环程序(2)在 S 上不可终止,则存在点 $X=X^*\in S$ 是其不可终止点.亦即对任意的非负整数 k,有 $A^kX^*\in S$.因此存在 $Y^*=PX^*\in \boldsymbol{P}(S)$,在迭代 k 次后变为 $Y_k=J^kY^*=PA^kP^{-1}Y^*$.又因为 $Y^*=PX^*$,故 $X^*=P^{-1}Y^*$.因此,$Y_k=PA^kX^*$.既然 $A^kX^*\in S$,故根据 $\boldsymbol{P}(S)$的定义知,$Y_k\in \boldsymbol{P}(S)$.因此,循环程序(3)在 $\boldsymbol{P}(S)$上也是不可终止的.

反过来,若循环程序(3)在 $\boldsymbol{P}(S)$上不可终止,则存在点 $Y=Y^*\in \boldsymbol{P}(S)$是其不可终止点.亦即对任意的非负整数 k,有 $Y_k=PA^kP^{-1}Y^*\in \boldsymbol{P}(S)$.既然 $Y^*\in \boldsymbol{P}(S)$,根据定义,必存在 $X^*\in S$,使得 $Y^*=PX^*$,故 $X^*=P^{-1}Y^*$.因此,$Y_k=PA^kX^*$.记 $X_k=A^kX^*$,则 $Y_k=PX_k\in \boldsymbol{P}(S)$.根据 $\boldsymbol{P}(S)$的定义,有 $X_k\in S$.因此,循环(2)在 S 上不可终止. □

注:既然 S 是有界闭的,且 P 为连续映射,故 $\boldsymbol{P}(S)$是有界闭的.

根据定理 2,判定循环程序(2)的终止性就等价于判定循环程序(3)的终止性.根据矩阵的 Jordan 标注型,将变元向量 Y 进行分块为 $Y=(\boldsymbol{y}_1,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_m)$,显然有:

$$|J^kY|^2=\left|\begin{pmatrix}J_1^k & & \\ & \ddots & \\ & & J_m^k\end{pmatrix}\begin{pmatrix}\boldsymbol{y}_1\\ \vdots\\ \boldsymbol{y}_m\end{pmatrix}\right|^2=\left|\begin{pmatrix}J_1^k\boldsymbol{y}_1\\ \vdots\\ J_m^k\boldsymbol{y}_m\end{pmatrix}\right|^2=\sum_{i=1}^{m}|J_i^k\boldsymbol{y}_i|^2 \tag{4}$$

根据公式(4),若存在某个 $|J_i^k\boldsymbol{y}_i|^2\to+\infty(k\to+\infty)$,则$|J^kY|^2\to+\infty$.为方便起见,下文中我们将用公式(1)中第 2 种类型的 Jordan 块统一表示这两种类型的 Jordan 块.亦即,当 D_i,I 都是 1×1 的矩阵时,则 $D_i\in R$,这时就变为第 1 种类型的 Jordan 块.由线性代数理论, J_i^k 显示地表示为

$$(J_i^k)_{r_i\times r_i}=\begin{pmatrix}D_i^k & kD_i^{k-1} & C_k^2D_i^{k-2} & \ldots & C_k^{r_i-1}D_i^{k-(r_i-1)}\\ 0 & D_i^k & kD_i^{k-1} & \ldots & C_k^{r_i-2}D_i^{k-(r_i-2)}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \ldots & D_i^k & kD_i^{k-1}\\ 0 & 0 & \ldots & 0 & D_i^k\end{pmatrix} \tag{5}$$

这里,r_i 是 Jordan 块 J_i 的维数; $C_{m_1}^{m_2}$ 为一组合数,且对 $m_1<m_2$,有 $C_{m_1}^{m_2}=0$.显然,若 D_i 为 2×2 矩阵时,将 $D_i=\rho_iM_i$ 代入到上式,则 J_i^k 的维数为 $2r_i$.不难看出, J_i^k 沿反对角线对称.记 ρ_i 为 J_i 的特征值的模,那么:

- 若 D_i,I 是 1×1 的矩阵时,即 $D_i=\lambda_i$,则$|D_i|=\rho_i=|\lambda_i|$,且有 $\boldsymbol{y}_i=(\boldsymbol{y}_{i,1},...,\boldsymbol{y}_{i,r_i})^T\in R^{r_i}$;
- 若 D_i,I 是 2×2 的矩阵时,则$|D_i|=\rho_i=|\alpha_i+i\beta_i|$,且 $\boldsymbol{y}_i=(\boldsymbol{y}_{i,11},\boldsymbol{y}_{i,12},...,\boldsymbol{y}_{i,r_i1},\boldsymbol{y}_{i,r_i2})^T\in R^{2r_i}$.

记$\Lambda_1=\{1,2,\ldots,r_i\}$,$\Lambda_2=\{11,12,21,22,\ldots,r_i1,r_i2\}$.

命题 3. 记号同上,则 $|J_i^k\boldsymbol{y}_i|^2=\rho_i^{2k}\sum_{v=0}^{2(r_i-1)}\boldsymbol{c}_v(\boldsymbol{y}_i,\rho_i)k^v$.

证明:将公式(5)代入到向量 $J_i^k\boldsymbol{y}_i$,有:

$$(J_i^k\boldsymbol{y}_i)=\begin{pmatrix}D_i^k\boldsymbol{y}_{i\mathbf{1}} & + & kD_i^{k-1}\boldsymbol{y}_{i\mathbf{2}} & + & C_k^2D_i^{k-2}\boldsymbol{y}_{i\mathbf{3}} & + & \ldots & + & C_k^{r_i-1}D_i^{k-(r_i-1)}\boldsymbol{y}_{i\boldsymbol{r_i}}\\ 0 & + & D_i^k\boldsymbol{y}_{i\mathbf{2}} & + & kD_i^{k-1}\boldsymbol{y}_{i\mathbf{3}} & + & \ldots & + & C_k^{r_i-2}D_i^{k-(r_i-2)}\boldsymbol{y}_{i\boldsymbol{r_i}}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & + & 0 & + & \ldots & + & D_i^k y_{i\boldsymbol{r_i-1}} & + & kD_i^{k-1}\boldsymbol{y}_{i\boldsymbol{r_i}}\\ 0 & + & 0 & + & \ldots & + & 0 & + & D_i^k\boldsymbol{y}_{i\boldsymbol{r_i}}\end{pmatrix} \tag{6}$$

这里,若 D_i 为 1×1 矩阵,则$\{1,2,\ldots,\boldsymbol{r_i}\}=\Lambda_1$;若 D_i 为 2×2 矩阵,则$\{1,2,\ldots,\boldsymbol{r_i}\}=\Lambda_2$,即,此时$\{1,2,\ldots,\boldsymbol{r_i}\}$中的每个元素都是二维向量.仅需注意到:矩阵 $J_i^k\boldsymbol{y}_i$ 中右上角的元素 $C_k^{r_i-1}D_i^{k-(r_i-1)}\boldsymbol{y}_{i\boldsymbol{r_i}}$ 中关于 k 的次数是最高的,为 r_i-1 次,因此,

$|J_i^k \boldsymbol{y}_i|^2$ 中关于 k 的最高次数为 $2(r_i-1)$.此外,若 D_i 是 1×1 的矩阵,则 $D_i=\lambda_i$.若从 J_i^k 中提取 λ_i^k ,则可从 $|J_i^k \boldsymbol{y}_i|^2$ 中提出 $|\lambda_i|^{2k}$.令 $\rho_i=|\lambda_i|$,命题成立;同理,若 D_i 是 2×2 的矩阵,则 $D_i^k=\rho_i^k M_i^k$,故可从 $|J_i^k \boldsymbol{y}_i|^2$ 中提出 ρ_i^{2k} ,命题也成立. □

根据命题 3 中的计算表达式,可以按字典序定义 $|J^k Y|^2$ 中各单项式的序为:如果 $\rho_i<\rho_j$,或 $\rho_i=\rho_j, u<v$,则,

$$\rho_i^k k^u \prec_{plex} \rho_j^k k^v .$$

由命题 3 可知,$|J_i^k \boldsymbol{y}_i|^2$ 中变化率最快的项为主导项.关于主导项的系数,有下列结论:

命题 4. 记号同上:

(1) 当 $|D_i|>1$ 且 $\boldsymbol{y}_i\neq 0$ 时,$|J_i^k \boldsymbol{y}_i| \to +\infty$;

(2) 当 $|D_i|<1$ 时,$|J_i^k \boldsymbol{y}_i| \to 0$;

(3) 当 $|D_i|=1$ 且 $\boldsymbol{y}_i$ 中后 $\boldsymbol{r}_i-1$ 个分量 $\boldsymbol{y}_{i,2},...,\boldsymbol{y}_{i,r_i}$ 不全为 0 时,$|J_i^k \boldsymbol{y}_i| \to +\infty$.

证明:根据线性代数理论,若给定矩阵 B 的所有特征值模都大于 1,则对任意非零 Y,有 $|B^k Y|\to+\infty$;若 B 的所有特征值模都小于 1,则对任意的 Y,有 $|B^k Y|\to 0$.故该命题的结论(1)、结论(2)显然成立.

下面证明结论(3)成立.由命题 3 的证明可知,$|J_i^k \boldsymbol{y}_i|^2$ 中主导项的系数来自于矩阵 $J_i^k \boldsymbol{y}_i$ 中的右上角的元素 $C_k^{r_i-1} D_i^{k-(r_i-1)} \boldsymbol{y}_{ir_i}$.因此,当 D_i 是 1×1 的矩阵时,从 $|J_i^k \boldsymbol{y}_i|^2$ 提出 $|\lambda_i|^{2k}$ 后,$C_k^{r_i-1} D_i^{k-(r_i-1)} \boldsymbol{y}_{ir_i}$ 中关于 k 的最高次项变为

$$\frac{k^{r_i-1}}{(r_i-1)!|\lambda_i|^{r_i-1}} \boldsymbol{y}_{ir_i} .$$

此时有 $\boldsymbol{r}_i=r_i$,则 $|J_i^k \boldsymbol{y}_i|^2$ 中含变化率最快的 $\rho_i^{2k} k^{2(r_i-1)}$ 项的系数:

$$c_{2(r_i-1)}=\left(\frac{1}{(r_i-1)!|\lambda_i|^{r_i-1}} \boldsymbol{y}_{i,r_i}\right)^2=\frac{1}{(r_i-1)!^2 \rho_i^{2(r_i-1)}}|\boldsymbol{y}_{i,r_i}|^2 .$$

当 D_i 是 2×2 的矩阵时,从 $|J_i^k \boldsymbol{y}_i|^2$ 提出 ρ_i^{2k} 后,$C_k^{r_i-1} D_i^{k-(r_i-1)} \boldsymbol{y}_{ir_i}$ 中关于 k 的最高次项变为

$$\frac{k^{r_i-1}}{(r_i-1)!\rho_i^{r_i-1}} M_i^{k-(r_i-1)} \boldsymbol{y}_{ir_i,r_i=\{r_i 1,r_i 2\}} .$$

因此,$|J_i^k \boldsymbol{y}_i|^2$ 中含 $\rho_i^{2k} k^{2(r_i-1)}$ 项的系数:

$$\boldsymbol{c}_{2(r_i-1)}(\boldsymbol{y}_i,\rho_i)=\left|\frac{1}{(r_i-1)!\rho_i^{r_i-1}} M_i^{k-(r_i-1)} \boldsymbol{y}_{ir_i}\right|^2=\frac{1}{(r_i-1)!^2 \rho_i^{2(r_i-1)}}|\boldsymbol{y}_{ir_i}|^2 .$$

上式中,既然 M 为旋转映射,其对向量 $\boldsymbol{y}_{ir_i}$ 作用不会改变向量的长度.因此,上式最后一个等号成立.综上所述,若 $\boldsymbol{y}_{i,r_i}\neq 0$,则 $|J_i^k \boldsymbol{y}_i| \to +\infty$.由公式(6)易知,若依次令 $\boldsymbol{y}_{i,r_i}=0, \boldsymbol{y}_{i,r_i-1}=0,..., \boldsymbol{y}_{i,3}=0, \boldsymbol{y}_{i,2}=0$,则 $|J_i^k \boldsymbol{y}_i|^2$ 中的主导项将依次为

$$\rho_i^{2k} k^{2(r_i-2)} \frac{1}{(r_i-2)!^2 \rho_i^{2(r_i-2)}}|\boldsymbol{y}_{i,r_i-1}|^2, \rho_i^{2k} k^{2(r_i-3)} \frac{1}{(r_i-3)!^2 \rho_i^{2(r_i-3)}}|\boldsymbol{y}_{i,r_i-2}|^2,..., \rho_i^{2k} k^2 \frac{1}{1!^2 \rho_i^2}|\boldsymbol{y}_{i,2}|^2, \rho_i^{2k}|\boldsymbol{y}_{i,1}|^2 .$$

既然 $\rho_i=|D_i|=1$,因此当 $\boldsymbol{y}_{i,r_i}, \boldsymbol{y}_{i,r_i-1},..., \boldsymbol{y}_{i,2}$ 不全为 0 时,有 $|J_i^k \boldsymbol{y}_i|^2 \to +\infty$. □

根据定理 5 可知,在满足一定条件下,循环程序(3)的终止性可归结为是否有不动点的判定.而不动点的计算是简单的,这使得循环程序(3)的终止性验证变得非常简便.

定理 5. 记号同上.若 J 中没有形如 $\lambda=-1, \lambda=\alpha+i\beta(|\lambda|=1, \beta\neq 0)$ 的特征值,则循环程序(3)是不可终止的,当且仅当 J 在 $\boldsymbol{P}(S)$ 中有不动点.

证明:若 J 在 $\boldsymbol{P}(S)$ 中有不动点,则程序显然不可终止.因此,下面证明若程序不可终止,则映射在 $\boldsymbol{P}(S)$ 中必有不动点.由题设,不失一般性,假设 J 中除了模不等于 1 的特征值外,还含有模为 1 的特征值 $\lambda=1$.既然 J 中的 Jordan 块的顺序可通过初等变换进行调整,因此不失一般性,令 $J=diag(J_{\rho>1}, J_{\rho=1}, J_{\rho<1})$.其中,$J_{\rho>1}, J_{\rho=1}, J_{\rho<1}$ 分别由 J 中特征值的模大于 1、等于 1、小于 1 的 Jordan 块构成的对角阵.根据 J 中 Jordan 块的顺序,变元向量 Y 也可被重写为 $Y=(Y_{\rho>1}, Y_{\rho=1}, Y_{\rho<1})^T$.这里,$Y_{\rho>1}, Y_{\rho=1}, Y_{\rho<1}$ 分别对应对角矩阵 $J_{\rho>1}, J_{\rho=1}, J_{\rho<1}$.若程序(3)是不可终止的,则必存在点

$Y^*=(Y^*_{\rho>1},Y^*_{\rho=1},Y^*_{\rho<1})$,使得无穷迭代序列 $\{J^kY^*\}_{k=0}^{\infty}\subseteq \boldsymbol{P}(S)$.因为

$$J^kY^*=diag(J^k_{\rho>1}Y^*_{\rho>1},J^k_{\rho=1}Y^*_{\rho=1},J^k_{\rho<1}Y^*_{\rho<1}).$$

由命题 4 以及公式(4)可知,假设 $Y^*_{\rho>1}\neq 0$,有 $|J^k_{\rho>1}Y^*_{\rho>1}|\to+\infty$,那么$|J^kY^*|\to+\infty$.因为 $\boldsymbol{P}(S)$是有界的,故必存在 k_o,有 $J^{k_o}Y^*\notin \boldsymbol{P}(S)$.这与 Y^*是不可终止点矛盾,故 $Y^*_{\rho>1}=0$.显然,$J_{\rho>1}\cdot 0=0$,故 $Y^*_{\rho>1}=0$ 为 $J_{\rho>1}$ 的不动点,故有:

$$J^k_{\rho>1}Y^*_{\rho>1}=Y^*_{\rho>1}=0.$$

因此在 Y^*中,对应于 $Y_{\rho>1}$ 的分量必须为 0,即 $Y^*_{\rho>1}=0$.同理,不妨记 $J_{\rho=1}=Diag(J_{v+1},\ldots,J_{v+u}),\boldsymbol{y}_{\rho=1}=(\boldsymbol{y}_{v+1},\ldots,\boldsymbol{y}_{v+u})$.同上述分析,由命题 4 的结论(3)可知,对任意的 $i=v+1,\ldots,v+u$,若 $\boldsymbol{y}_{i,2},\ldots,\boldsymbol{y}_{i,r_i}$ 不全为 0,则 $|J^k_i\boldsymbol{y}_i|\to+\infty$,从而导致 $|J^kY^*|\to+\infty$.因此在 Y^*中,对应于 $\boldsymbol{y}_{i,2},\ldots,\boldsymbol{y}_{i,r_i}$,$i=v+1,\ldots,v+u$ 的分量 $\boldsymbol{y}^*_{i,2}=\ldots=\boldsymbol{y}^*_{i,r_i}=0$,即 $\boldsymbol{y}^*_i=(\boldsymbol{y}^*_{i,1},0,\ldots,0)^T$,不难看出:

$$J_i\cdot\boldsymbol{y}^*_i=\boldsymbol{y}^*_{i,1}\cdot J_i\cdot e_1=\boldsymbol{y}^*_{i,1}\cdot e_1=\boldsymbol{y}^*_i.$$

这里,$e_1=(1,0,\ldots,0)^T$,$i=v+1,\ldots,v+u$.显然,对任意的 $i=v+1,\ldots,v+u$,$\boldsymbol{y}^*_i$ 为 J_i 的不动点,故有 $J^k_i\boldsymbol{y}^*_i=\boldsymbol{y}^*_i$.最后,当 $k\to+\infty$,$J^k_{\rho<1}Y^*_{\rho<1}\to 0$.显然,0 是 $J_{\rho<1}$ 的不动点.综上所述,当 $k\to+\infty$时,序列 J^kY^*趋近于 J 的不动点.既然 $\boldsymbol{P}(S)$是有界闭的,故其中收敛点列的极限点必在 $\boldsymbol{P}(S)$中,因此该不动点必在 $\boldsymbol{P}(S)$中. □

注:由命题 4 及定理 5 的证明可知,若 $Y=(Y_{\rho>1},Y_{\rho=1},Y_{\rho<1})^T$ 为循环(3)不可终止点,则必有 $Y_{\rho>1}=0,Y_{\rho=1}=(\boldsymbol{y}_{v+1},\ldots,\boldsymbol{y}_{v+u})^T,\boldsymbol{y}_i=(\boldsymbol{y}_{i,1},0,\ldots,0)^T,i=v+1,\ldots,v+u$.

推论 6. 记号同上.若 A 中没有特征值$\lambda=-1,\lambda=\alpha+i\beta(|\lambda|=1,\beta\neq 0)$,则循环程序(2)是不可终止的,当且仅当 A 在 S 中有不动点.

证明:若 $X^*\in S$ 为 A 的不动点,即 $AX^*=X^*$,因为 $A=P^{-1}JP$,故 $JPX^*=PX^*$.根据 $\boldsymbol{P}(S)$的定义可知,令 $Y^*=PX^*\in\boldsymbol{P}(S)$,显然,$Y^*$为 J 在 $\boldsymbol{P}(S)$的不动点;反之,若 $Y^*\in\boldsymbol{P}(S)$为 J 的不动点,即 $JY^*=Y^*$,则由 $\boldsymbol{P}(S)$的定义,必存在 $X^*\in S$,有 $Y^*=PX^*$.因此 $JPX^*=PX^*$,故 $AX^*=X^*$.因此,A 在 S 中有不动点,等价于 J 在 $\boldsymbol{P}(S)$中有不动点.根据定理 2 和定理 5 得知结论成立. □

根据命题 4 中的结论(1)、结论(3)可知,当变元 Y 中对应于特征值模大于 1 的 Jordan 块的分量不全为 0,或者变元 Y 中对应于特征值模等于 1 的 Jordan 块中除第 1 列外的其余分量不全为 0 时,当 $k\to+\infty$时,有$|J^kY|\to+\infty$,此时,程序(3)必终止.记 Y 中对应这上述两种情形的变元分量的集合为 $\boldsymbol{z}_0$,则根据定理 5 中的证明可知,循环(3)的不可终止点中,对应于 $\boldsymbol{z}_0$ 的分量均为 0,故循环(3)的不可终止性仅与 Y 中的其余分量 $\boldsymbol{z}_1=Y/\boldsymbol{z}_0$ 有关.

令 $Y=\boldsymbol{z}_0\cup\boldsymbol{z}_1$,置 $\boldsymbol{z}_0$ 中的变元为 0,即 $\boldsymbol{z}_0=0$.记超平面 $L:\boldsymbol{z}_0=0$.令Θ为有界闭集 $\boldsymbol{P}(S)$与超平面 L 相交形成的截面,显然,Θ是 $R^{n-|z_0|}$ 中的有界闭集.记 $J'=diag(1_l,M_1,\ldots,M_s,J_{\rho<1})$,其中,$1_l$ 表示由 l 个±1 构成的集合.J'中对角线上的元素±1 为 J 中特征值为±1 的 Jordan 块的第 1 行第 1 列的元素,对角线 $M_1,\ldots,M_s$ 为 J 中特征值的模为 1 但特征值不等于 1 的 Jordan 块的第 1 行第 1 列的元素,对角线上其余元素为 J 中特征值为小于 1 的 Jordan 块.令 $Y'\cup\boldsymbol{z}_1$ 表示 Y',$\boldsymbol{z}_1$ 含有相同的变元,我们有下面的结论:

命题 7. 记号同上.循环程序(3)是不可终止的当且仅当程序(7):

$$\left.\begin{array}{c}\textbf{while } Y'\in\Theta \textbf{ do}\\ \{Y'=J'Y'\}\\ \textbf{endwhile}\end{array}\right\} \tag{7}$$

是不可终止的.

证明:根据上面的分析可知,针对循环(3),若变元向量 Y 中对应于 $\boldsymbol{z}_0$ 中的分量至少有一个不为 0,即 $\boldsymbol{z}_0\neq 0$,则循环(3)必然终止.因此,若循环(3)不终止,不妨记 Y^*为循环(3)的不可终止点,则 Y^*中对应于 $\boldsymbol{z}_0$ 的分量 $\boldsymbol{z}^*_0=0$,即

$$Y^*=(0_{\rho>1},\boldsymbol{y}^*_{v_1},\ldots,\boldsymbol{y}^*_{v_{l+s}},Y^*_{\rho<1})^T\in\boldsymbol{P}(S).$$

这里,$\boldsymbol{y}^*_{v_i}=(\boldsymbol{y}^*_{v_i,1},0,\ldots,0)^T,i=1,\ldots,l+s$,对应于特征值的模为 1 的 Jordan 块 $J_{v_1},\ldots,J_{v_{l+s}}$.则

$$J^kY^*=(J^k_{\rho>1}Y^*_{\rho>1},J^k_{\rho=1}Y^*_{\rho=1},J^k_{\rho<1}Y^*_{\rho<1})^T=(0_{\rho>1},J^k_{v_1}\boldsymbol{y}^*_{v_1},\ldots,J^k_{v_{l+s}}\boldsymbol{y}^*_{v_{l+s}},J^k_{\rho<1}Y^*_{\rho<1})^T\in\boldsymbol{P}(S) \tag{8}$$

既然 $J_{v_1},...,J_{v_{l+s}}$ 的特征值的模为 1,那么对任意的 i=1,…,l+s,若 J_{v_i} 的特征值 $\lambda_{v_i}=1$,则 $J_{v_i}^k\boldsymbol{y}_{v_i}^*=(\boldsymbol{y}_{v_i}^*,0,...,0)^T$ (不动点);若 $\lambda_{v_i}=-1$,则 $J_{v_i}^k\boldsymbol{y}_{v_i}^*=(\pm\boldsymbol{y}_{v_i}^*,0,...,0)^T$ (2-周期点);若 J_{v_i} 的特征值 $\lambda_{v_i}\neq\pm1$,则 $J_{v_i}^k\boldsymbol{y}_{v_i}^*=(M_{v_i}^k\cdot\boldsymbol{y}_{v_i,1}^*,0,...,0,0)^T$. 因此,$J^kY^*$中的分量要么为 0,要么为 $\pm\boldsymbol{y}_{v_i}^*,M_i^k\cdot\boldsymbol{y}_{v_i,1}^*$ 或 $J_{\rho<1}^kY_{\rho<1}^*$.不妨设 J 中 l+s 个模为 1 的特征值中λ=±1 的特征值有 l 个,$\lambda\neq\pm1$ 的特征值有 s 个,既然 J 中 Jordan 块的位置可以通过初等变换进行调整,那么可将对角阵 $J_{\rho=1}$ 中对应于特征值为±1 的 Jordan 块排在前面,而特征值不为±1 的 Jordan 块排在后面.

不失一般性,令 $Y'^*=(\boldsymbol{y}_{i_1}^*,...,\boldsymbol{y}_{i_l1}^*,\boldsymbol{y}_{j_1,1}^*,...,\boldsymbol{y}_{j_s,1}^*,Y_{\rho<1}^*)^T$,显然,$Y'^*\in\Theta$.又

$$J'^kY'^*=(\boldsymbol{y}_{i_1}^*,...,\boldsymbol{y}_{i_l1}^*,M_{j_1}^k\cdot\boldsymbol{y}_{j_1,1}^*,...,M_{j_s}^k\cdot\boldsymbol{y}_{j_s,1}^*,J_{\rho<1}^kY_{\rho<1}^*)^T,$$

既然 $J^kY^*\in\boldsymbol{P}(S)\cap L$,故 $J'^kY'^*\in\Theta$.因此,循环(7)在 Y'^*处不可终止.最后我们证明:若循环(7)不可终止,则循环(3)也不可终止.这是显然的.因为若循环(7)在点 Y'^*处不可终止,由于 $Y'=\boldsymbol{z}_1,Y=\boldsymbol{z}_0\cup\boldsymbol{z}_1=\boldsymbol{z}_0\cup Y'$,则点 Y^*(其对应于 $\boldsymbol{z}_0$ 的分量取为 0,对应于 $\boldsymbol{z}_1$ 的分量 $\boldsymbol{z}_1=Y'^*$)必是循环(3)的不可终止点. □

根据命题 7,要判定循环(3)的终止性,等价于判定循环(7)的终止性.循环(7)中的赋值映射是由±1 和 2×2 的旋转映射以及特征值模小于 1 的 Jordan 块构成的对角阵.其中,M_i 可写为 $M_i(\theta_i),\theta_i=2\pi\alpha_i,i=1,...,s$.因此,

$$M_i(\theta_i)\square\ \mathrm{e}^{\alpha_i\cdot2\pi i},\boldsymbol{i}=\sqrt{-1}.$$

特别地,对任意的 i=1,2,…,s,若 $\alpha_i=\dfrac{\theta_i}{2\pi}\in Q$(有理数),则当 $k\to+\infty,\mathrm{e}^{k\cdot\alpha_i2\pi i}$ 的值将在圆周上呈周期变化.因此,对所有的 i=1,…,s,可以找到 $\mathrm{e}^{\alpha_i2\pi i}$ 的公共周期 T.例如,当 $s=2,\alpha_1=\dfrac{1}{2},\alpha_2=\dfrac{1}{3}$,则 $\mathrm{e}^{\alpha_12\pi i},\mathrm{e}^{\alpha_22\pi i}$ 的公共周期 T=6.因此,当 $k\to+\infty$,点 $(\mathrm{e}^{k\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{k\cdot\alpha_s\cdot2\pi i})$ 必在下列点上周期变化:

$$(\mathrm{e}^{Tk\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{Tk\cdot\alpha_s\cdot2\pi i}),(\mathrm{e}^{(Tk+1)\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{(Tk+1)\cdot\alpha_s\cdot2\pi i}),(\mathrm{e}^{(Tk+2)\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{(Tk+2)\cdot\alpha_s\cdot2\pi i}),...,(\mathrm{e}^{(Tk+T-1)\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{(Tk+T-1)\cdot\alpha_s\cdot2\pi i}).$$

又因为 $\mathrm{e}^{(Tk+t)\cdot\alpha_i\cdot2\pi i}=\mathrm{e}^{t\cdot\alpha_i\cdot2\pi i},t=0,1,...,T-1$,故当 $k\to+\infty$,点 $(\mathrm{e}^{k\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{k\cdot\alpha_s\cdot2\pi i})$ 必在下列点上周期变化:

$$(1,...,1),(\mathrm{e}^{1\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{1\cdot\alpha_s\cdot2\pi i}),(\mathrm{e}^{2\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{(2\cdot\alpha_s\cdot2\pi i}),...,(\mathrm{e}^{(T-1)\cdot\alpha_1\cdot2\pi i},...,\mathrm{e}^{(T-1)\cdot\alpha_s\cdot2\pi i}).$$

令 $M=diag(M_1(\alpha_12\pi),M_2(\alpha_22\pi),...,M_s(\alpha_s2\pi)),\alpha_i\in Q$,既然 $M_i(\theta_i)\square\ \mathrm{e}^{\alpha_i\cdot2\pi i}$,因此,

$$M_i^{Tk+j}(\theta_i)\square\ \mathrm{e}^{(Tk+j)\alpha_i\cdot2\pi i}=\mathrm{e}^{j\alpha_i\cdot2\pi i}\square\ M_i^j(\theta_i),j=0,...,T-1.$$

因此,

$$M^{Tk+j}=M^j=diag(M_1(j\cdot\alpha_12\pi),...,M_s(j\cdot\alpha_s2\pi)),j=0,...,T-1.$$

根据上述分析可得,任给 $Y_M=(\boldsymbol{y}_1,...,\boldsymbol{y}_s)^T\neq0,\boldsymbol{y}_i\in R^2$,有:

$$M\cdot Y_M=(M_1(\alpha_12\pi)\boldsymbol{y}_1,M_2(\alpha_22\pi)\boldsymbol{y}_2,...,M_s(\alpha_s2\pi)\boldsymbol{y}_s).$$

特别地,当$\alpha_i\in Q,i$=1,…,s,无穷迭代序列:

$$\left.\begin{aligned}\{M^k\cdot Y_M\}_{k=0}^{\infty}=\{&(\boldsymbol{y}_1,...,\boldsymbol{y}_s),\\&(M(1\cdot\alpha_12\pi)\boldsymbol{y}_1,...,M(1\cdot\alpha_s2\pi)\boldsymbol{y}_s),...,\\&(M((T-1)\cdot\alpha_12\pi)\boldsymbol{y}_1,...,M((T-1)\cdot\alpha_s2\pi)\boldsymbol{y}_s)\}\end{aligned}\right\}\tag{9}$$

即,

$$\{M^kY_M\}_{k=0}^{\infty}=\{M^{Tk}Y_M\}_{k=0}^{\infty}\cup\{M^{Tk+1}Y_M\}_{k=0}^{\infty}\cup...\cup\{M^{Tk+T-1}Y_M\}_{k=0}^{\infty}\tag{10}$$

为方便起见,J'可被写为 $J'=diag(1_l,M,J_{\rho<1}),M=\{M_1,...,M_s\}$.即,$J'$中有 l 个值为±1 的实特征值,s 个模为 1 的型如$\alpha+i\beta(\beta\neq0)$的复特征值.因此,$J'$中有 l+s 个模为 1 的特征值.

命题 8. 记号同上.若$\alpha_1,\alpha_2,...,\alpha_s$均为有理数,则循环程序(7)是不可终止的,等价于映射 J'在Θ中存在周期轨或不动点.

证明:若 J'在Θ中有周期轨(或不动点),即 $Ord_{Y^*}=\{Y^*,J'(Y^*),...,J'^{T-1}(Y^*)\}\subset\Theta(1\leqslant T<+\infty)$,则程序(7)显然是不可终止的.因此,下面仅证明:当$\alpha_1,\alpha_2,...,\alpha_s$均为有理数时,循环程序(7)是不可终止的,则必在$\Theta$中有一条周期轨或不动点.因为$\alpha_1,\alpha_2,...,\alpha_s$均为有理数,故记 T 为 $\{\mathrm{e}^{\alpha_i\cdot2\pi i}\}_{i=1}^s$ 的公共周期.若循环程序(7)是不可终止的,则必然存在

一点 $Y'^*\in\Theta$,使得 $\{J'^kY'^*\}_{k=0}^{\infty}\subseteq\Theta$.根据 J'中的分块, $Y'^*=(\boldsymbol{y}_{1_l}^*,\boldsymbol{y}_M^*,\boldsymbol{y}_{\rho<1}^*)^T,\boldsymbol{y}_M^*=(\boldsymbol{y}_1^*,...,\boldsymbol{y}_s^*),\boldsymbol{y}_i^*\in R^2$,因此,

$$J'^kY'^*=(\boldsymbol{y}_{1_l}^*,M^k\boldsymbol{y}_M^*,J_{\rho<1}^k\boldsymbol{y}_{\rho<1}^*).$$

若无特征值−1 且 $\boldsymbol{y}_M^*=0$,则当 $k\to+\infty$, $J_{\rho<1}^k\boldsymbol{y}_{\rho<1}^*\to 0$,故 $J'^kY'^*\to Y^o=(\boldsymbol{y}_{1_l}^*,0,...,0)^T\in\Theta$.显然,Y^o 为循环(7)的不动点.若有特征值−1 且 $\boldsymbol{y}_M^*\neq 0$,则记新的周期 T 为 2 与$\alpha_1,\alpha_2,\ldots,\alpha_s$ 的公共周期 T 的最小公倍数,即 T=*Lcm*(T,2).因此,序列$\{J^kY^*\}$可被分为至多 T 个不同的子序列,即

$$\{J'^kY'^*\}=\{J'^{Tk}Y'^*\}_{k=0}^{\infty}\cup\{J'^{Tk+1}Y'^*\}_{k=0}^{\infty}\cup...\cup\{J'^{Tk+T-1}Y'^*\}_{k=0}^{\infty}.$$

根据公式(9),当 $k\to+\infty$时,

$$J'^{Tk+j}Y'^*\to(\boldsymbol{y}_{1_{\lambda=1}}^*,M(j\cdot\alpha_1 2\pi)\boldsymbol{y}_1^*,...,M(j\cdot\alpha_s 2\pi)\boldsymbol{y}_s^*,0,...,0)^T=\hat{Y}_j,j=0,...,T-1.$$

因为Θ是有界闭的,故其中收敛序列的极限点必在Θ中,即 $\hat{Y}_j\in\Theta$.显然, $Ord_{Y^*}=\{\hat{Y}_0,...,\hat{Y}_{T-1}\}$ 为Θ中的一条长度不超过 T 的周期轨. □

根据命题 8 的证明,我们回到循环程序(3)的终止性分析,有下面的结论成立:

定理 9. 记号同上.若 A 的所有模为 1 的特征值的辐角均为π的有理倍,则循环程序(2)是不可终止的,当且仅当 A 在 S 中有不动点或周期轨.

证明:这个证明类似于命题 8 中的证明,限于篇幅此处省略. □

根据定理 9,若矩阵 A 中含有模为 1 的特征值 $\eta_i=\mathrm{e}^{\alpha_i 2\pi i}$,则需要判定其辐角是否为π的有理倍,即判定是否$\alpha_i\in Q$.文献[17]中呈现了一个方法去判定一个特征值$\eta$的幅角是否为π的有理倍,并找到其周期.

2 实 例

例 1:考虑下列循环的终止性:

$$\left.\begin{array}{c}\textbf{while }(x-5)^2+(y-6)^2-\sqrt[3]{y}-\sqrt{xy}\leqslant 2\,||\,-5\leqslant x\leqslant -1\,\&\&\,1\leqslant y\leqslant 7\textbf{ do}\\ \begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-1 & 2\\ \frac{1}{7} & \frac{1}{3}\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\\ \textbf{endwhile}\end{array}\right\}\tag{11}$$

记 S 为循环条件围成的有界闭域,既然循环条件通过运算符&&,||联立得到,且表达式含根式,故文献[17]的方法已不能处理.通过计算,矩阵 A 有两个实特征值$\xi_1\approx 0.5211599258$,$\xi_2\approx -1.18782692$.它们的模都不为 1,故满足推论 6 的题设,计算其不动点为$(0,0)\notin S$.根据命题 6,该循环可终止.

例 2:考虑下列程序的终止性:

$$\left.\begin{array}{c}\textbf{while }\ 1\leqslant x^2+y^2\leqslant 20\ \textbf{ do}\\ \begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0 & 2\\ -\frac{1}{2} & -1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\\ \textbf{endwhile}\end{array}\right\}\tag{12}$$

循环条件围成的区域 S 是有界闭集.通过计算,A 有一对模为 1 的共轭复特征值为

$$\xi_1=-\frac{1}{2}+\frac{\sqrt{3}}{2}\boldsymbol{i},\xi_2=-\frac{1}{2}-\frac{\sqrt{3}}{2}\boldsymbol{i}.$$

这两个特征值较为特殊,可以看出两个幅角 $\theta_1=\frac{1}{3}\cdot 2\pi,\theta_2=-\frac{1}{3}\cdot 2\pi$. 因此, $\alpha_1=-\alpha_2=\frac{1}{3}\in Q$. 其公共周期为 T=3,这里不必使用文献[17]的方法来判定两个特征值的幅角是否为π的有理倍.故满足定理 9 的题设.因此,根据定理 9,若循环不终止,则 A 在 S 中必有不动点或长度至多为 3 的周期轨.因此,通过计算,其不动点为$(0,0)\notin S$.而对任意的非零点 $X^*\neq 0$ 均为其 3-周期点.通过计算半代数系统:

$$\{X\in S:AX\neq X,A^2X\neq X,A^3X=X\}\cap\{X\in S:AX\in X,A^2X\in X,A^3X\in X\},$$

可以判定是否在 S 中存在 3-周期轨,通过计算得到点 $X^*=(-1,2)^T$,使得:

$$Ord_{X^*}=\left\{(-1,2),\left(4,-\frac{3}{2}\right),\left(-3,-\frac{1}{2}\right)\right\}\subset S.$$

故程序不可终止.

上述几个例子中的循环区域 S 很容易看出都是有界闭的,但倘若 S 的有界性不易看出,则可将 S 的有界性判定问题转化为下列等价的量词公式:

$$\exists r>0,\forall X\in S\Rightarrow\|X\|<r \tag{13}$$

这里,$\|X\|$表示向量 X 的欧氏范数.对公式(14),可使用符号计算中的柱形代数分解技术进行判定.

3 结 论

本文研究了有界闭域上的带线性赋值的循环程序终止性问题,证明了在满足给定条件下,该类程序的终止性是可判定的,并给出了简明的判定方法.尽管我们的分析中借助了矩阵的 Jordan 标准型,但循环终止性的判定却并不需要做 Jordan 标准型计算.相较于文献[17],本文有两方面不同:首先,在研究的程序类型上,文献[17]中所研究的循环程序,其循环条件必须是由&&联立多个多项式表达式而成.与文献[17]中研究的程序类型不同,本文研究的程序类型的循环条件并不必为多项式表达式(本文中,程序的循环条件中可含有根式、超越函数),且循环条件也可由几个表达式经过&&,||运算符联立构成,因此扩大了终止性可判定的程序类型范围;其次,二者在终止性判定方法上不同.为方便,以下面简单例子来阐述两者方法的不同:

$$\left.\begin{array}{c}\textbf{while } 1\leqslant(x-4)^2+y^2\leqslant 3 \textbf{ do}\\ \begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}1&0\\2&5\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\\ \textbf{endwhile}\end{array}\right\} \tag{14}$$

首先,我们采用文献[17]的方法来判定其终止性,其过程包括以下几个步骤:

(1) 计算 $X(n)=A^nX(0)$.这里,$X(n)$表示初始点 $X(0)=(x(0),y(0))^T$ 在 n 次迭代后的显示表达式.但该表达式在文献[17]的计算极大地依赖于赋值矩阵 A 的特征值的精确计算,而这等价于精确计算 A 的特征多项式的根.但这是很困难的,因为 5 次或 5 次以上的单变元方程的根一般不能被精确计算出来.由于例 2 中的赋值矩阵较简单,不难精确计算出它的两个特征值:$\xi_1=1,\xi_2=5$.因此,根据文献[17]的方法,得到 $X(n)$的表达式为

$$X(n)=(x(n),y(n))^T=\left(x,-\frac{1}{2}x+\frac{1}{2}x5^n+y5^n\right)^T \tag{15}$$

(2) 将公式(15)代入到循环条件中,得:

$$Cond(n)=\frac{5}{4}x^2-8x+15-\frac{x^2}{2}5^n-xy5^n+\frac{x^2}{4}25^n+25^nxy+25^ny^2\geqslant 0\ \&\&$$
$$\frac{5}{4}x^2-8x-\frac{x^2}{2}5^n-xy5^n+\frac{x^2}{4}25^n+25^nxy+25^ny^2\leqslant -13.$$

因此,要判定循环(14)是否可终止,等价于判定在循环条件形成的圆环域 S 中是否存在一点(x,y),使得对某个正整数 N,当 $n>N$,时,有 $Cond(n)$中的两个不等式均成立.这依赖于两个不等式中各单项式随 n 的变化率.因此,可将 $Cond(n)$中两个不等式的各单项式按变换率快慢排序,得到:

$$Cond(n)=\left(\frac{x^2}{4}+xy+y^2\right)25^n+\left(-\frac{x^2}{2}-xy\right)5^n+\frac{5}{4}x^2-8x+15\geqslant 0\ \&\&$$
$$-\left(\frac{x^2}{4}+xy+y^2\right)25^n-\left(-\frac{x^2}{2}-xy\right)5^n-\frac{5}{4}x^2+8x-13\geqslant 0.$$

令

$$s_{\mu 1}=\{(x,y):\mu_1>0\},s_{\mu 2}=\{(x,y):\mu_1=0,\mu_2>0\},s_{\mu 3}=\{(x,y):\mu_1=\mu_2=0,\mu_3\geqslant 0\},$$
$$s_{\nu 1}=\{(x,y):\nu_1>0\},s_{\nu 2}=\{(x,y):\nu_1=0,\nu_2>0\},s_{\nu 3}=\{(x,y):\nu_1=\nu_2=0,\nu_3\geqslant 0\},$$

其中,

$$\mu_1=\frac{x^2}{4}+xy+y^2,\mu_2=-\frac{x^2}{2}-xy,\mu_3=\frac{5}{4}x^2-8x+15,$$
$$\nu_1=-\left(\frac{x^2}{4}+xy+y^2\right),\nu_2=-\left(-\frac{x^2}{2}-xy\right),\nu_3=-\frac{5}{4}x^2+8x-13.$$

(3) 要判断是否存在一点(x,y),使得对任意的 $n>N$,都有 $Cond(n)$中的两个不等式均成立,需要求解下列 9 个半代数系统是否有解:$s_{\mu i}\cap s_{\nu j},i,j=1,2,3$.倘若有解,则循环(14)不可终止;否则终止.通过计算可得,这 9 个半代数系统均无解,故循环(14)可终止.

下面运用本文方法来判定该循环的终止性.不难看出,循环(14)满足本文推论 6 的题设,因此根据推论 6,要判断其终止性,仅需判定在循环条件形成的圆环域 s 中是否有不动点即可.通过简单计算可知,其映射的不动点为直线 l:$x+2y=0$ 上的点.从图像上易知,直线 l 与 s 并不相交,因此在圆环域 s 中没有不动点,故该循环可终止.当然,该结论也可通过判定一个半代数系统$\{(x,y):1\leqslant(x-4)^2+y^2\leqslant 3\wedge AX=X\}$是否为空来得到.通过计算,该半代数系统为空(无解),故循环可终止.

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作者的建设性意见;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). [doi: 10.3969/j.issn.1000-8217.2008.03.005]

[2] Yang L, Zhou C, Zhan N, Xia B. Recent advances in program verification through computer algebra. Frontiers of Computer Science, 2012,4(1):1−16. [doi: 10.1007/s11704-009-0074-7]

[3] Colón MA, Sipma HB. Practical methods for proving program termination. In: Proc. of the LNCS, Vol.2404. Heidelberg: Springer, 2002. 227−240.

[4] Podelski A, Rybalchenko A. A complete method for the synthesis of linear ranking functions. In: Proc. of the VMCAI. 2004. 239−251. [doi: 10.1007/978-3-540-24622-0_20]

[5] Bradley AR, Manna Z, Sipma HB. Linear ranking with reachability. In: Proc. of the CAV. LNCS 3576, 2005. 491−504. [doi: 10.1007/11513988_48]

[6] Cousot P. Proving program invariance and termination by parametric abstraction, Langrangian relacation 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]

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

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

[9] Gupta AK, Henzinger TA, Majumdar R, Rybalchenko A, Xu RG. Proving non-termination. In: Proc. of the POPL. 2008. 147−158. [doi: 10.1145/1328438.1328459]

[10] 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]

[11] 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]

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

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

[14] Xu M, Chen LY, Zeng ZB, Li ZB. Termination analysis of linear loops. Int'l Journal of Foundations of Computer Science, 2010, 21(6):1005−1019. [doi: 10.1142/S0129054110007696]

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

[16] Yao Y. Termination of nonlinear programs over intervals. Ruan Jian Xue Bao/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]

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

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]

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

[16] 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]

李轶(1980－),男,重庆人,博士,副研究员,CCF 会员,主要研究领域为程序验证,符号计算.
E-mail: zm_liyi@163.com

吴文渊(1976－),男,博士,副研究员,主要研究领域为同伦计算.
E-mail: wuwenyuan@cigit.ac.cn

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.
E-mail: yongfeng@cigit.ac.cn