软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(2):297−304 [doi: 10.13328/j.cnki.jos.004782]

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

多分支单变量循环程序的终止性分析*

李 轶[1], 李传璨[1,2], 吴文渊[1]

[1](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)

[2](重庆邮电大学 计算机科学与技术学院,重庆 400065)

通讯作者: 李轶, E-mail: zm_liyi@163.com

摘 要: 对多分支单变量循环程序的终止性问题进行了研究.证明了在适定的条件下,该类循环程序不可终止性的充分必要条件是迭代映射在循环条件形成的区域中有不动点.特别地,当这类循环程序是多项式循环程序时,在给定条件下,其在实数域上的终止性问题是可判定的.

关键词: 可信计算;多分支循环程序;终止性分析

中图法分类号: TP311

中文引用格式: 李轶,李传璨,吴文渊.多分支单变量循环程序的终止性分析.软件学报,2015,26(2):297−304. http://www.jos.org.cn/1000-9825/4782.htm

英文引用格式: Li Y, Li CC, Wu WY. Termination analysis of multipath loop programs with one variable. Ruan Jian Xue Bao/Journal of Software, 2015,26(2):297−304 (in Chinese). http://www.jos.org.cn/1000-9825/4782.htm

Termination Analysis of Multipath Loop Programs with One Variable

LI Yi[1], LI Chuan-Can[1,2], WU Wen-Yuan[1]

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

[2](College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Termination of multipath loop programs with one variable is analyzed in this paper. It demonstrates that under proper conditions, this kind of loops is non-terminate if and only if there exist fixed points. Especially, if the class of programs are polynomial, then under proper conditions, the termination of the programs is decidable over the reals.

Key words: trusted computing; multipath loop program; termination analysis

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,而作为嵌入式系统灵魂的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:可达性、终止性、不变式.可达性是指一个系统能否从一个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;不变式则是系统变量在循环迭代时永远保持的特性;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[1],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[2],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.当程序的秩函数被找到时,则表明程序是可终止的.

* 基金项目: 国家自然科学基金(61103110); 重庆市科技攻关项目(cstc2012ggB40004, cstc2013jjys0002)
收稿时间: 2014-07-02; 修改时间: 2014-10-31; 定稿时间: 2014-11-26

利用多面体理论和整数规划等代数方法,国外科学家在线性秩函数的合成方面取得了大量成果[3−7].此外,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(非线性)多项式型不变式和秩函数生成的方法[1,8,9].不同于文献[10]中的方法,他们的方法能够精确判定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.即,可以构造一个循环程序,它是可终止的,但并没有秩函数.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.从可判定的角度进行终止性研究的结果甚少.2004 年,Tiwari 在文献[11]中首次证明了下列循环程序在实数域上的终止性是可判定的:

$$\boldsymbol{Q}_1\ \textbf{While}\ BX>0\ \textbf{do}$$

$$\{X:=AX\}$$

这里,$A,B\in R^{n\times n},X\in R^n$ 相似的结论被 Braveman[12]推广到整数环上.此外,为避免 Jordan 标准型的浮点计算,文献[13]中提出了精确的符号计算方法对程序进行终止性判定.2010 年,文献[14]对程序的终止性进行了分析,证明了当程序满足给定的 NZM(non-zero minimum)条件时的终止性是可判定的:

$$\boldsymbol{Q}_2\ \textbf{While}\ P(X)>0\ \textbf{do}$$

$$\{X:=AX\}$$

其中,$P(X)$为(非线性)多项式.从可判定的角度,目前的研究多集中于单重循环程序的终止性分析,而针对带多分支语句的循环终止性分析结果甚少.2005 年,Bradley 等人[15]研究了一类多分支多项式循环程序的终止性问题.他们的方法极大地依赖于循环程序中表达式的有限差分树结构,并建立了不完备的判定方法.但大多数循环程序并没有有限差分树结构,因而限制了该方法的使用.

本文中,我们对一类带多个分支的单变量循环程序的终止性问题进行了分析.证明了当满足所给定的条件时,这类循环不可终止的充分必要条件为迭代映射在循环条件形成的区域中有不动点.倘若我们将这类循环中的表达式都限定为多项式表达式(这类循环称为多分支单变量多项式循环程序),那么在满足给定条件下,根据由 Tarski 提出的一阶多项式公式的真伪是可判定的这一结论可知,这类多分支单变量多项式循环程序在实数域上的终止性问题是可判定的.针对多分支单变量多项式循环程序,文中定理给定的条件非常容易借助实代数工具 QEPCAD 和 DISCOVERER 去验证.不同于 Bradley 等人的方法,本文呈现的方法并不需要循环程序具有有限差分树的结构.

1 主要结果

下文中,我们称由迭代函数 F 和循环条件形成的区域 I 所构成的循环程序 $P(F,I)$在实数域$\mathbb{R}$是不可终止的,如果存在一点 $x_0\in\mathbb{R}$,使得 $\{F^i(x_0)\}_{i=0}^{+\infty}\subseteq I$.这里,$F^i=F\circ F\circ\ldots\circ F$ 表示函数的复合.如果那样的 x_0 不存在,则称循环 $P(F,I)$在实数域上可终止.

定理 1. 令 $f:R\mapsto R$ 为一维连续映射.I 为一闭区间.循环程序

$$\boldsymbol{P}_1\ \textbf{While}\ x\in I\ \textbf{do}$$

$$\{x:=f(x)\}$$

是不可终止的充分必要条件为迭代映射 f 在闭区间 I 上有不动点.

证明:充分性.如果 f 在 I 上有不动点,则程序 P_1 显然不可终止.

必要性.若 f 在 I 上没有不动点,则由函数的连续性可知:必存在正数 $c>0$,使得对任意的 $x\in I$,有 $f(x)-x\geqslant c>0$;或者,必存在正数 $c>0$,使得对任意的 $x\in I$,$f(x)-x\leqslant -c<0$.下面我们将分两种情况证明程序 P_1 必然终止.

(1) 存在正数 $c>0$,使得对任意的 $x\in I$,有 $f(x)-x\geqslant c>0$.任取一点 $x_0\in I$,由 x_0 将产生一无穷迭代序列:$\{f^n(x_0)\}_{n=0}^{\infty}$.

下面将证明必存在一正整数 k,使得迭代序列中的点 $f^k(x_0)\notin I$.假设这样的 k 不存在,那么有 $\{f^n(x_0)\}_{n=0}^{\infty}\subseteq I$;又因为存在正数 $c>0$,使得对任意的 $x\in I$,$f(x)-x\geqslant c>0$,则有:

$$x_0\leqslant f(x_0)-c\leqslant f^2(x_0)-2c\leqslant\ldots.$$

因此,在有限步后,迭代序列 $\{f^n(x_0)\}_{n=0}^{\infty}$ 中的点将跳出区间 I.假设不成立,这样的 k 必然存在,即,在情形(1)中,程序 P_1 必然可终止.

(2) 存在正数 $c>0$,使得对任意的 $x\in I$,有 $f(x)-x\leqslant -c<0$.类似于情形(1)的分析,同理可证明:对任意的 $x_0\in I$,必存在正整数 k,使得 $f^k(x_0)\notin I$.即,程序 P_1 在 I 上可终止.综上所述,f 在 I 上没有不动点时,程序 P_1 可终止. □

记循环程序:

P_2 **While** $x\in I$ **do**
{
if $x\in I_1$ **then** $x:=f_1(x)$
else if $x\in I_2$ **then** $x:=f_2(x)$
…
else if $x\in I_{n-1}$ **then** $x:=f_{n-1}(x)$
else $x:=f_n(x)$
}

这里,$f_i:R\mapsto R$ 为一维连续映射.令

$$F(x)=\begin{cases} f_1(x), x\in I_1\\ f_2(x), x\in I_2\\ \vdots\\ f_n(x), x\in I_n \end{cases}.$$

令 $I=\bigcup_{i=1}^{n} I_i$ 为一闭区间,且 $I_i\cap I_j=\varnothing(\forall i\neq j)$.根据上述记号,程序 P_2 可被重写为

P_2 **While** $x\in I$ **do**
$\{x:=F(x)\}$

定理 2. 记号同上.记 D_I, D_{I_i} 分别为区间 I, I_i 的端点集合.令 $D^o=\bigcup_{i=1}^{n} D_{I_i}\setminus D_I$.如果满足以下条件,那么,程序 P_2 是不可终止的的充分必要条件为迭代映射 F 在闭区间 I 上有不动点:

(1) 存在正数 $\delta>0$,使得对任意的 $x\in I$ 都有: $F(x)\notin\bigcup_{e\in D^o} O(e,\delta)$.

(2) 存在$\mathbb{R}$上的连续函数 $T(x)$,使得下列分段函数:

$$G(x)=T\circ F-T=\begin{cases} T\circ f_1(x)-T(x), x\in I_1\\ T\circ f_2(x)-T(x), x\in I_2\\ \vdots\\ T\circ f_n(x)-T(x), x\in I_n \end{cases} \tag{1}$$

在闭区间 I 上连续,且满足(3).

(3) 对任意的 $x\in I$,有 $G(x)=0\Rightarrow F(x)-x=0$(即,对任意的 $x\in I_i$,有 $T\circ f_i(x)-T(x)=0\Rightarrow f_i(x)-x=0, i=1,2,\ldots,n$).

证明:充分性.若 F 在 I 上有不动点,则程序 P_2 不可终止.

必要性.若程序 P_2 不可终止,必存在无穷迭代序列 $\Delta=\{x_0,F(x_0),F^2(x_0),\ldots\}\subseteq I$.令 $T(\Delta)=\{T(F^i(x_0))\}_{i=0}^{\infty}$.因为 T 连续,故数列 $T(\Delta)$有界,记其上、下确界分别为 $T_\perp, T_\top$.分两种情形:

(A) 若 $T_\perp\in T(\Delta)$,则必存在 $x_t=F^t(x_0)\in\Delta\subseteq I\setminus\bigcup_{e\in D^o} O(e,\delta)$,有 $T(x_t)=T_\perp\in T(\Delta)$.令 $x_\perp=x_t$.故存在 $x_\perp\in\Delta$,有: $T(F(x_\perp))\leqslant T(x_\perp)$.

(B) 若 $T_\perp\notin T(\Delta)$,则由确界性质可知:必存在子列 $\{T(F^{n_k}(x_0))\}_{k=0}^{\infty}$ 收敛于 $T_\perp$,也即 $\lim_{k\to+\infty} T\circ F^{n_k}(x_0)=T_\perp$.又因为数列 $\{F^{n_k}(x_0)\}_{k=0}^{\infty}\subseteq I$ 有界,故必有收敛子列 $\{F^{n_{k_v}}(x_0)\}_{v=0}^{\infty}$.即

$$\lim_{v\to+\infty} F^{n_{k_v}}(x_0)=x^*.$$

因为由题设可知:存在正数 $\delta>0$,使得对任意的 $x\in I$ 都有 $F(x)\notin\bigcup_{e\in D^o} O(e,\delta)$, 故 $x^*\in I\setminus\bigcup_{e\in D^o} O(e,\delta)$. 由

T 的连续性可知:

$$\lim_{v\to+\infty} T\circ F^{n_{k_v}}(x_0)=T\lim_{v\to+\infty} F^{n_{k_v}}=T(x^*);$$

且因为 $\{T\circ F^{n_{k_v}}(x_0)\}_{v=0}^{\infty}$ 为收敛数列 $\{T(F^{n_k}(x_0))\}_{k=0}^{\infty}$ 的子列,故有 $T(x^*)=T_\perp$.令 $x_\perp=x^*\in I\setminus\bigcup_{e\in D^o}O(e,\delta)$.

因为 $T_\perp$ 为 $T(\Delta)$的上确界,故对任意的 n,有 $T\circ F^n(x_0)\leqslant T_\perp=T(x_\perp)$.因此有:

$$T\circ F^{n_{k_v}+1}(x_0)=T\circ F\circ F^{n_{k_v}}(x_0)<T_\perp=T(x_\perp) \tag{2}$$

因为 F 在 $I\setminus\bigcup_{e\in D^o}O(e,\delta)$ 上连续,故,

$$\lim_{v\to+\infty} T\circ F\circ F^{n_{k_v}}(x_0)=T\lim_{v\to+\infty} F\circ F^{n_{k_v}}(x_0)=T\circ F\lim_{v\to+\infty} F^{n_{k_v}}(x_0)=T\circ F(x^*)=T\circ F(x_\perp).$$

因此,对公式(2)两边取极限,有 $T\circ F(x_\perp)\leqslant T(x_\perp)$.

综上所述,无论情形(A)或情形(B),均可得到一点 $x_\perp\in I\setminus\bigcup_{e\in D^o}O(e,\delta)$, 使得 $T\circ F(x_\perp)\leqslant T(x_\perp)$.

同理,对下确界 $T_\top$,采用完全类似的分析可知,必存在一点 $x_\top\in I\setminus\bigcup_{e\in D^o}O(e,\delta)$,使得 $T\circ F(x_\top)\geqslant T(x_\top)$.

又因为由题设中的条件(2)可知:函数 $G(x)=TF(x)-T(x)$在 I 上连续,且 $T\circ F(x_\perp)\leqslant T(x_\perp)$, $T\circ F(x_\top)\geqslant T(x_\top)$,故必存在 $\hat{x}\in I$, 使得 $G(\hat{x})=0$. 根据题设中的条件(3)可知,必有 $F(\hat{x})=\hat{x}$. 故, $\hat{x}$ 为 F 在 I 上不动点. □

注:因为迭代函数 F 在闭区间上是不连续的,而题设条件(2)中辅助函数 $T(x)$的引入便于构造闭区间上的连续函数.要检验定理中的条件(2)是否成立,即检验函数 $G(x)$是否为 I 上的连续函数,仅需验证 $G(x)$在相邻两个区间端点的函数值是否相等.比如,假设两个相邻区间为 $I_j=(a_j,b_j)$,$I_{j+1}=[a_{j+1},b_{j+1}]$,$b_j=a_{j+1}$.$G(x)$要在 I 上连续,必须满足 $G(b_j)=G(a_{j+1})$.辅助函数 $T(x)$的构建是关键.在实际的计算中,我们无法事先知道辅助函数 T 的具体表达式.为了计算出 T,我们需要先给出 T 的一个参系数模板(为了便于计算,文中我们选用了多项式模板).然后,通过工具 DISCOVERER 和 QEPCAD,我们得到了参系数的取值范围 $\phi(a,b,\ldots)$(这里,$a,b,\ldots$为模板中的参系数).$\phi(a,b,\ldots)$是一个由多项式等式或不等式构成的半代数系统.如果这个系统 $\phi(a,b,\ldots)$非空,即,存在 $a,b,\ldots$的某个取值 $a^*,b^*,\ldots$满足 $\phi(a,b,\ldots)$,则满足题设的函数 T 被构造出来;否则,若 $\phi(a,b,\ldots)$为空,则我们需要修改 T 的模板再重新计算.因此,若系统 $\phi(a,b,\ldots)$非空,则 T 的选择是很多的,甚至是无穷多种选择.

定理 2 的结论可以推广到更加一般的情形.首先给出一些记号.

令 $\hat{I}_1,\ldots,\hat{I}_n$ 为 n 个闭区间, $\hat{F}_i$ 为定义在闭区间 $\hat{I}_i$ 上的函数.这里, $\hat{F}_i\in\{f_i,F_i\}$ 且 f_i,F_i 分别型如程序 P_1,P_2 中的迭代映射.若 $\hat{F}_i\triangleq f_i$, 则表明 $\hat{F}_i$ 为闭区间 $\hat{I}_i$ 上一个连续函数;若 $\hat{F}_i\triangleq F_i$, 则表明 $\hat{F}_i$ 为闭区间 $\hat{I}_i$ 上一个逐段连续函数.

令 $\overline{[1,n]}=\{1,2,\ldots,n\}$, 根据定义的不同类型的迭代函数,$n$ 个闭区间可被分为两类:

$$\Lambda_1=\{i\in\overline{[1,n]}:\hat{F}_i\triangleq f_i\},\Lambda_2=\{i\in\overline{[1,n]}:\hat{F}_i\triangleq F_i\}.$$

对任意的 $i\in\Lambda_2$,记 $\hat{I}_i=\bigcup_{j=1}^{k_i}I_{ij}$, 且对任意的 $j,j'=1,\ldots,k_i$,有 $I_{ij}\cap I_{ij'}=\varnothing$.同时,对任意的 $i\in\Lambda_2$,记 $D_{\hat{I}_i}$,$D_{I_{ij}}$ 分别为区间 $\hat{I}_i,I_{ij}$ 的端点集合.令 $D_i^o=\bigcup_{j=1}^{k_i}D_{I_{ij}}\setminus D_{\hat{I}_i},i\in\Lambda_2$, 令 x_L,x_R 分别为闭区间 $\hat{I}_1,\ldots,\hat{I}_n$ 中最小的左端点和最大的右端点,且令 $\hat{I}=[x_L,x_R]$. 显然, $\bigcup_{i=1}^{n}\hat{I}_i\subseteq\hat{I}$. 同时,令 $\hat{I}_i\subseteq\hat{I}_i',\hat{I}_i'\cap\hat{I}_j'=\varnothing,\bigcup_{i=1}^{n}\hat{I}_i'=\hat{I}$.

令

$$\begin{aligned}&\boldsymbol{P}_3\ \textbf{While}\ x\in\bigcup_{i=1}^{n}\hat{I}_i\ \textbf{do}\\&\{x:=\hat{F}(x)\}\end{aligned}$$

这里,

$$\hat{F}(x)=\begin{cases}\hat{F}_1(x),x\in\hat{I}_1\\\hat{F}_2(x),x\in\hat{I}_2\\\vdots\\\hat{F}_n(x),x\in\hat{I}_n\end{cases}.$$

定理 3. 记号同上.如果满足以下条件,那么,程序 P_3 是不可终止的的充分必要条件为迭代映射 $\hat{F}$ 在 $\bigcup_{i=1}^{n}\hat{I}_i$ 上有不动点:

(1) 存在正数δ>0,使得对任意的 $x\in\bigcup_{i=1}^{n}\hat{I}_i$, 都有: $\hat{F}(x)\notin\bigcup_{e\in(\bigcup_{i\in\Lambda_2}D_i^o)}O(e,\delta)$.

(2) 存在$\mathbb{R}$上的连续函数 $T(x)$,使得下列分段函数:

$$G(x)=T\circ\hat{F}-T=\begin{cases}T\circ\hat{F}_1(x)-T(x),x\in\hat{I}_1'\\T\circ\hat{F}_2(x)-T(x),x\in\hat{I}_2'\\\vdots\\T\circ\hat{F}_n(x)-T(x),x\in\hat{I}_n'\end{cases}\tag{3}$$

在闭区间 $\hat{I}$ 上连续,即,对任意的 i, $T(\hat{F}_i(x))-T(x)$ 在区间 $\hat{I}_i'$ 上连续;且对任意两个相邻区间 $\hat{I}_i',\hat{I}_{i+1}'$, $T(\hat{F}_i(x))-T(x)$ 在区间 $\hat{I}_i'$ 右端点的函数值等于 $T(\hat{F}_{i+1}(x))-T(x)$ 在区间 $\hat{I}_{i+1}'$ 左端点的函数值.且满足:

(3) 任意的 $x\in\bigcup_{i=1}^{n}\hat{I}_i'$,有 $G(x)=0\Rightarrow\hat{F}(x)-x=0$.即,对任意的 $x\in\hat{I}_i$, 有:

$$T\circ\hat{F}_i(x)-T(x)=0\Rightarrow\hat{F}_i(x)-x=0,\ \ i=1,2,\ldots,n.$$

(4) $G(x)$在 $\hat{I}\setminus\bigcup_{i=1}^{n}\hat{I}_i$ 上没有零点.

证明:这个证明非常类似于定理 2 的证明.若 $\hat{F}$ 在 $\bigcup_{i=1}^{n}\hat{I}_i$ 上有不动点,则程序 P_3 显然不可终止.假设程序 P_3 不可终止,类似于定理 3 中的证明,题设中的条件(1)、条件(2)保证了在 $\bigcup_{i=1}^{n}\hat{I}_i$ 中必然存在两点 $x_\top,x_\perp$,使得:

$$G(x_\top)\geqslant 0,\ G(x_\perp)\leqslant 0.$$

因此,根据 G 在 $\hat{I}$ 上的连续性可知:必在 $\hat{I}$ 上存在一点 $\hat{x}\in\hat{I}$, 有 $G(\hat{x})=0$.

根据题设中的条件(4)可知, $\hat{x}\in\bigcup_{i=1}^{n}\hat{I}_i$. 再根据条件(3),即得 $\hat{F}(\hat{x})=\hat{x}$. □

定理 1~定理 3 将一类多分支单变量循环程序在实数域上的终止性问题等价地规约为判定其赋值函数在循环条件中的区间上是否有实的不动点的问题.这里,各定理中的赋值函数仅要求连续即可.因此,连续赋值函数表达式的复杂多样性导致不动点的计算变得困难.但是,倘若我们将赋值函数限定为多项式,则区间上不动点是否存在的判定问题等价于一个半代数系统有无实数解的判定问题.后者可以用一阶多项式公式来描述,进而根据 Tarski 的结论可知该问题是可判定的.同时,既然循环中所有表达式均为多项式的,那么定理中各题设条件的验证问题均可等价转换为半代数系统有无实解的问题.由上述分析可知,后者是可判定的.因此,由上述分析,我们有以下显然的结论:

定理 4. 在满足定理 1~定理 3 的题设条件下,型如 P_1,P_2,P_3 的多分支单变量多项式循环程序在实数域上的终止性是可判定的.

下面,我们给出几个具体的多项式循环程序来阐述本文的方法.

2 实 例

例 1:考虑下列循环的终止性:

While $-3\leqslant x\leqslant 1$ **do**

$\{x:=11x^6+41x^5+2x^4-7x^3-21x^2+15x-71\}$

迭代函数 f 在循环条件[−3,1]上没有不动点,由定理 1 可知,该循环必然终止.既然定理 1 中仅需要迭代函数为连续函数,那么定理 1 对下列循环仍然适用:

例 2:考虑下列循环的终止性:

While $-3\leqslant x\leqslant 5$ **do**

{

if $-5\leqslant x<0$ **then** $x:=-4x+2$

else if $0\leqslant x\leqslant 1$ **then** $x:=2x^3+2$

else if $1<x<3$ **then** $x:=x^2+3x$

else x:=7x−3

}

不难验证,相邻两端段函数在间断点处的函数值均相等,故迭代函数在区间[−5,5]连续.迭代函数在循环条件[−5,5]上没有不动点,由定理 1 可知,该循环必然终止.

例 3:考虑下列循环的终止性:

While $x^2\leqslant 4$ **do**

{

if $0<x\leqslant 2$ **then** x:=$-x^2-1$

else x:=$2x^2+x+1$

}

令 $f_1=-x^2-1$,$f_2=2x^2+x+1$.显然,$-1=f_1(0)\neq f_2(0)=1$.故迭代函数在 $x=0$ 处不连续,因此定理 1 对该循环不再适用.我们将利用定理 2 对该循环的终止性进行判定.根据定理 2 的题设,需要首先验证 3 个条件是否满足.记循环条件围成的闭区间为 $I=[-2,2]$,两分支条件确定的区间分别为 $I_1=(0,2)$,$I_2=[-2,0]$.那么由定义可得:

$$D_I=\{-2,2\},D_{I_1}=\{0,2\},D_{I_2}=\{0,-2\},D^o=(D_{I_1}\cup D_{I_2})\setminus D_I=\{0\}.$$

令
$$F(x)=\begin{cases}f_1(x)=-x^2-1, & x\in I_1\\ f_2(x)=2x^2+x+1, & x\in I_2\end{cases}.$$

首先验证定理 2 中的条件(1)是否满足,这等价于判定下列量词公式是否成立:

$$\exists\delta\forall x((x\in I\wedge\delta>0)\Rightarrow(F(x)\geqslant\delta\vee F(x)\leqslant-\delta)).$$

通过工具 QEPCAD 可以判定上述公式成立.由此可知:对任意的 $x\in I$,$F(x)$都不会位于间断点 $x=0$ 的某一δ邻域内.即,定理 2 中条件(1)得到满足.

其次,为验证该循环是否满足定理 2 中条件(2)、条件(3),构造$\mathbb{R}$上的连续函数 $T(x)$.令 $T(x)=ax^2+bx$,$a,b\in\mathbb{R}$为参数.根据定理 2 中的公式(1),可构造函数 $G(x)$.为保证 $G(x)$在区间 I 内连续,只需使得 $G(x)$在 I 内唯一间断点 $x=0$ 处连续,即,需要满足:

$$T\circ f_1(0)-T(0)=T\circ f_2(0)-T(0) \tag{4}$$

根据公式(4),可得参数约束 $b=0$.即,当且仅当 $b=0$ 时,公式(4)成立.同时,为验证定理 2 中的条件(3)是否被满足,等价于验证下列系统无解:

$$x^2-4\leqslant 0\wedge G(x)=0\wedge F(x)-x\neq 0 \tag{5}$$

利用实代数工具 DISCOVERER 中的命令求解公式(5),即,

- *tofind*([$T\circ f_1(x)-T(x)$],[$2-x$],[x],[$f_1(x)-x$],[x],[a,b],0);
- *tofind*([$T\circ f_2(x)-T(x)$],[$x+2,-x$],[·],[$f_2(x)-x$],[x],[a,b],0).

得到如下参数 a,b 的约束:

$$(3a-b)(3a-4b)>0\wedge(a+2b)(5a+b)>0 \tag{6}$$

结合前面得到的约束 $b=0$,求解所有参数约束可得到 $a=1$,$b=0$.故定理 2 题设中的连续函数 $T(x)$存在.

综上所述,定理 2 中的 3 个条件都满足,根据定理 2,该循环不可终止的充要条件是迭代函数 F 在 I 上有不动点.经过计算,迭代函数 F 在 I 上没有不动点,故该循环可终止.

例 4:考虑下列循环的终止性:

While $-2\leqslant x\leqslant -1\vee 1\leqslant x\leqslant 2$ **do**

{

if $-2\leqslant x\leqslant -1$ **then** x:=$-2x^2-4x+1$

else $x:=-\frac{11}{5}x^2+x+9$

}

该循环条件由两个闭区间构成,故定理 1、定理 2 均不适用.

根据定理 3 中的记号,令 $\hat{I}_1=[-2,-1],\hat{I}_2=[1,2],\hat{I}=[-2,2]$,记:

$$\hat{F}(x)=\begin{cases}\hat{F}_1\triangleq f_1(x)=-2x^2-4x+1, & x\in\hat{I}_1\\ \hat{F}_2\triangleq f_2(x)=-\dfrac{11}{5}x^2+x+9, & x\in\hat{I}_2\end{cases}.$$

下面验证定理 3 中的条件是否被满足.

首先,既然$\Lambda_2=\varnothing$,那么定理 3 中的条件(1)自然成立.

其次,构造连续函数 $T(x)=ax^2+bx$,并由此构建型如公式(3)的连续函数 $G(x)$.

取 $\hat{I}_1'=[-2,0],\hat{I}_2'=(0,2],\hat{I}_1'\cap\hat{I}_2'=\varnothing$,显然有 $\hat{I}_1\subseteq\hat{I}_1',\hat{I}_2\subseteq\hat{I}_2',\hat{I}_1'\cup\hat{I}_2'=\hat{I}$.

因此,$G(x)$要在 $\hat{I}$ 上连续,必须满足 $T\circ\hat{F}_1(0)-T(0)=T\circ\hat{F}_2(0)-T(0)$. 由此得到参数约束:

$$b=-10a \tag{7}$$

当公式(7)成立时,定理 3 中的条件(2)得到满足.为了满足定理 3 中的条件(3),等价于下列系统无实数解:

$$-2\leqslant x\leqslant -1\wedge T\circ f_1(x)-T(x)=0\wedge f_1(x)-x\neq 0 \tag{8}$$

$$1\leqslant x\leqslant 2\wedge T\circ f_2(x)-T(x)=0\wedge f_2(x)-x\neq 0 \tag{9}$$

调用 *tofind* 命令,可以得到参数约束:

$$(a-b)(2a+b)<0\wedge(44a+5b)(21a+5b)>0 \tag{10}$$

令 $\hat{I}\setminus\bigcup_{i=1}^{2}\hat{I}_i=(-1,1)$. 最后,要满足定理 3 中的条件(4),等价于下列系统无实数解:

$$-1<x\leqslant 0\wedge T\circ f_1(x)-T(x)=0 \tag{11}$$

$$0<x<1\wedge T\circ f_2(x)-T(x)=0 \tag{12}$$

调用 *tofind* 命令,可以得到参数约束:

$$(a+b)(17a+8b)>0\wedge(44a+5b)(104a+11b)>0 \tag{13}$$

根据参数约束(7)、参数约束(10)和参数约束(13),可得到 $a=1,b=-10$.因此,存在连续函数 $T(x)=x^2-10x$,满足定理 3 的所有条件.故根据定理 3,仅需计算其不动点是否在循环条件中来判定该循环的终止性.通过计算得知,$\hat{F}$ 在 $\hat{I}_1\cup\hat{I}_2$ 上没有不动点,故该循环可终止.

3 结 论

尽管循环程序的终止性问题被证明是不可判定的,但寻找可判定的程序子类并建立相应的判定算法具有重要的实际意义.本文对一类单变量多分支 while 循环程序的终止性问题进行了研究,证明了在给定条件下,这类循环程序不可终止的充要条件是迭代函数在循环条件形成的区域中有不动点.特别地,当这类循环程序为多项式循环程序时,证明了在适定条件下,该类多项式循环程序在实数域上的终止性问题是可判定的.本文方法的特点是:针对这类多分支单变量多项式循环程序,各个定理中的条件易于判定,即,容易通过实代数工具去验证定理中的条件是否成立;其次,判定不动点是否落入到循环条件形成的区域中的问题也可以转换为半代数系统求解,后者同样容易通过实代数工具进行判定.

致谢 感谢上海高可信计算重点实验室对本文工作的支持.

References:

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

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

[3] 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, 2013. 51−62. [doi: 10.1145/2429069.2429078]

[4] Colón MA, Sipma HB. Practical methods for proving program termination. In: Brinksma E, Larsen KG, eds. Proc. of the Computer Aided Verification. Berlin, Heidelberg: Springer-Verlag, 2002. 227−240. [doi: 10.1007/3-540-45657-0_36]

[5] Colón MA, Sipma HB. Synthesis of linear ranking functions. In: Margaria T, Wang Y, eds. Proc. of the 7th Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems. London: Springer-Verlag, 2001. 67−81. [doi: 10.1007/3-540-45319-9_6]

[6] 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]

[7] Podelski A, Rybalchenko A. A complete method for the synthesis of linear ranking functions. In: Steffen B, Levi G, eds. Proc. of the Verification, Model Checking, and Abstract Interpretation. Berlin, Heidelberg: Springer-Verlag, 2004. 239−251. [doi: 10.1007/978-3-540-24622-0_20]

[8] Chen YH, Xia BC, Yang L, Zhan NS, Zhou CC. Discovering non-linear ranking functions by solving semi-algebraic systems. In: Jones CB, Liu ZM, Woodcock J, eds. Proc. of the Theoretical Aspects of Computing (ICTAC 2007). Berlin, Heidelberg: Springer-Verlag, 2007. 34−49. [doi: 10.1007/978-3-540-75292-9_3]

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

[10] Cousot P. Proving program invariance and termination by parametric abstraction Langrangian relaxation and semidefinite programming. In: Cousot R, ed. Proc. of the Verification, Model Checking, and Abstract Interpretation. Berlin, Heidelberg: Springer-Verlag, 2005. 1−24. [doi: 10.1007/978-3-540-30579-8_1]

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

[12] Braverman M. Termination of integer linear programs. In: Ball T, Jones RB, eds. Proc. of the Computer Aided Verification. Berlin, Heidelberg: Springer-Verlag, 2006. 372−385. [doi: 10.1007/11817963_34]

[13] 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]

[14] 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]

[15] Bradley A, Manna Z, Sipma H. Termination of polynomial programs. In: Cousot R, ed. Proc. of the Verification, Model Checking, and Abstract Interpretation. Berlin, Heidelberg: Springer-Verlag, 2005. 113−129. [doi: 10.1007/978-3-540-30579-8_8]

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.

吴文渊(1976－),男,博士,副研究员,主要研究领域为同伦计算.

李传璨(1989－),男,硕士生,主要研究领域为程序验证.