Signature-based Method of Deciding Program Termination

Yaohui Li

Tianjin University of Technology and Education

October 24, 2012

Outline

- Introduction
- Determination of Positiove Eigenvalue
- Positivity of Eigenvector
- Experimental Result
- Conclusion

Introduction

- In recent years, mathematician and computer scientist apply computer algebra to program termination.
- Yong Cao, et al use Wu's characteristic set method and mathematical induction to prove the correctness of recursive program.
- Nikolaj Popov, Tudor Jebelean use computer algebra techniques for the specification, verification and synthesis of recursive programs.
- Lu Yang, et al reduce program verification to semi-algebraic system , then use DISCOVERER to isolate real roots so as to analyze termination or reachability of the program.

Introduction

- To avoid real root isolation, this paper converts program termination to the existence of real zeros in polynomial. Program termination is decided by counting sign changes of discriminant sequence. However, this method is inefficient because of many determinants computation in it. Hence, we use Gröbner basis method to improve the construction of sign list of positive real eigenvalue which satisfies $\mathbf{c}^{\mathbf{T}}\mathbf{v} > 0$. The algorithm is implemented by using symbolic computation and the experiment results demonstrate its correctness.

Determination of Positive Eigenvalue

- Considering the linear program of the following form

$$P : while(\mathbf{c}^T\mathbf{x} > 0)\{\mathbf{x} := A\mathbf{x}\} \tag{1}$$

  where $\mathbf{x} \in R^n$, $\mathbf{c} = \{c_i | c_i \in \mathbf{R}\}$ is $N \times 1$ vector and $A = (a_{ij}) \in R$ is a $M \times N$ matrix.
- Theorem[Tiwari]. If the linear loop program P, defined by an $(N \times N)$ matrix A and a nonzero $N \times 1$-vector $\mathbf{c}$, is nonterminating then there exists a real eigenvector $\mathbf{v}$ of A, corresponding to positive eigenvalue, such that $\mathbf{c}^T\mathbf{v} \geq 0$.

Determination of Positive Eigenvalue

Let $F(x) \in R(x)$ with $F(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$ and $G(x)$ be another polynomial. Then, $R(x)$ and M are as follows:

$$R(x) = rem(F'G, F) = b_1x^{m-1} + \cdots + b_m.$$

$$M = \begin{pmatrix}
a_0 & a_1 & a_2 & \cdots & a_m & & \\
0 & b_1 & b_2 & \cdots & b_m & & \\
 & a_0 & a_1 & a_2 & \cdots & a_m & \\
 & 0 & b_1 & b_2 & \cdots & b_m & \\
 & & & \vdots & \vdots & \vdots & \\
 & & a_0 & a_1 & a_2 & \cdots & a_m \\
 & & 0 & b_1 & b_2 & \cdots & b_m
\end{pmatrix}$$

Determination of Positive Eigenvalue

- Given a sign list $[s_1, s_2, \cdots, s_n]$, if $[s_i, s_{i+1}, \cdots, s_{i+j}]$ is a section of it, where $s_i \neq 0$, $s_{i+1} = s_{i+2} = \cdots = s_{i+j-1} = 0, s_{i+j} \neq 0$, then, we replace the subsection $[s_{i+1}, s_{i+2}, \cdots, s_{i+j-1}]$ by $[-s_i, -s_i, s_i, s_i, -s_i, -s_i, si, si, -s_i, \cdots]$, i.e. , $\varepsilon_{i+r} = (-1)^{\lfloor (r+1)/2 \rfloor} \cdot s_i$ for $r = 1, 2, \cdots, j-1$. Otherwise, $\varepsilon_k = s_k$. The new list is called as revised sign list(RSL).
- Yang proved the following theorem:
  Theorem[Yang]. Given real coefficient polynomials $F = F(x)$ and $G = G(x)$, if the sign changes number of $RSL(F, G)$ is n and $D_\eta \neq 0$ but $D_t = 0$ $(t > \eta)$, then $\eta - 2n = \#F_{G_+} - \#F_{G_-}$.

Determination of Positive Eigenvalue

where

$$\#F_{G_+} = card(\{x \in \mathbf{R} | F(x) = 0, G(x) > 0\}),$$
$$\#F_{G_-} = card(\{x \in \mathbf{R} | F(x) = 0, G(x) < 0\}).$$

- Base on the theorem, we check the existence of positive eigenvalue
  First, get the characteristic polynomial from matrix A and assume it is $F(x)$.
  Second, compute its derivative $F'(x)$ according to the method above.
  Third, construct $R(x) = Rem(F'(x)G(x), F(x))$(Do not discuss the selection of G(x) temporarily)

Determination of Positive Eigenvalue

- Four, use Maple to generate Bezout matrix of polynomials $F(x)$ and $R(x)$ and obtain RSL from the matrix.
- Finally, according to theorem 2(Yang) to compute the signature so as to check the existence of positive eigenvalue.
- Now we talk about selection of $G(x)$
  In order to decide the number of positive eigenvalue, select three different functions as $G(x)$.
  (1)Let G(x)=1. The value of $G(x)$ has nothing to do with x, the total number of real zeros is decided.
  (2)Let G(x)=x. The difference between the number of positive eigenvalue and that of negative ones is decided.

Determination of Positive Eigenvalue

- (3)Let $G(x) = x^2$. $G(x) > 0$ holds no matter what positive or negative eigenvalue is. In this case, we decide the number of eigenvalue which is not 0.
  Therefore, there is
  $$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} \#F_{x_=} \\ \#F_{x_>} \\ \#F_{x_<} \end{pmatrix} = \begin{pmatrix} m-2n \\ m-2n' \\ m-2n'' \end{pmatrix},$$
  Furtherly, we derive
  $$\begin{pmatrix} \#F_{x_=} \\ \#F_{x_>} \\ \#F_{x_<} \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} m-2n \\ m-2n' \\ m-2n'' \end{pmatrix}. \qquad (2)$$

Determination of Positive Eigenvalue

where $m = max(deg(F), deg(R))$ and it is order of Bezout matrix, n, n', n'' are the sign change numbers when $G(x) = 1, x, x^2$ respectively.
If $m = 2n'' or \# F_{x_+} = m - (n' + n'') = 0$ means there is no positive eigenvalues, then program P is terminating.
Disadvantage: In order to to compute the sequence of principal minors, we have to compute the determinant of different size for sign list.

Improvement

- According to the definition of Bezoutian, D is as follows:

  $$\frac{f(x)r(y)-f(y)r(x)}{x-y} = \sum_{i,j=1}^{m} b_{ij}x^{i-1}y^{j-1} = \begin{pmatrix} 1 & x & \cdots & x^{m-1} \end{pmatrix} (b_{ij}) \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{m-1} \end{pmatrix},$$

  where (b_{ij}) is $M \times M$ matrix produced by coefficients b_{ij}, it is called as Bezout matrix. One of its properties is symmetric.
- The discriminant matrix D of A is a real symmetric.Hence, all eigenvalues of D are real according to the theory in linear algebra. Therefore, we can use signature method to check the number of positive real zeros directly.

Improvement

- Theorem: The symbols are defined as above. Let D be discriminant matrix of $F(x)$ with respect to $G(x)$, its characteristic polynomial $cp(t)$. The difference σ between the number of sign changes of $cp(t)$ and $cp(-t)$ satisfies

$$\sigma(cp) = \#F_{G_+} - \#F_{G_-}.$$

- Advantage: According to this theorem, we needn't compute the determinant of submatrix of D for constructing revised Sturm list RSL.

Improvement

The procedure of checking positive eigenvalue:

- Construct discriminant matrix D;(same with the method before)
- Obtain the characteristic polynomial $cp(t)$ of D;
- Count the number of sign changes in $cp(t)$ and $cp(-t)$, compute the signature $\sigma(cp)$.

Note

Similar to formula (2), in order to get the number of positive eigenvalues of A, G has to be assigned $1, x, x^2$ respectively.

Positivity of Eigenvectors

The method in section (2) is only suitable to decide whether there is positive eigenvalue in $\mathbf{A}$. However, if positive eigenvalue exists, we have to check the existence of those eigenvector $\mathbf{v}$ such that $\mathbf{c}^T\mathbf{v} > 0$. Only such a condition satisfies, then can we decide that the program P is nonterminating. To solve this problem, we introduce Gröbner basis in the program verification.

Definition

In matrix A of program P, if there exists eigenvector $\mathbf{v}$ such that $\mathbf{c}^T\mathbf{v} > 0$, then we call it as positive eigenvector.

Positivity of Eigenvectors

- Consideration from the angle of mathematics, the main body $\mathbf{x} := \mathbf{A}\mathbf{x}$ in program P is equivalent to $(\mathbf{A} - \lambda\mathbf{E})\mathbf{x} = 0$. Hence, the eigenvector of A is the solution of the main body. "there exists a real eigenvector $\mathbf{v}$ of A, corresponding to positive eigenvalue, such that $\mathbf{c}^T\mathbf{v} \geq 0$" is equivalent to check whether those solutions which correspond to positive eigenvalues satisfy the constraint condition, i.e., the condition in while loop. On the base of this, we further to check the existence of positive eigenvector.

Positivity of Eigenvectors

In this case, the decidability of program P is equivalent to

$$\begin{cases} (\mathbf{A} - \lambda \mathbf{E})\mathbf{x} = 0, \\ \lambda > 0, \\ \mathbf{cx} > \mathbf{0} \end{cases}$$

Because we introduce new variable λ, the system becomes n linear equations with $n + 1$ variables. However, as the system is homogenous, the solution of eigenvector is sure on the unit ball, therefore we add $x_1^2 + \cdots + x_n^2 - 1 = 0$ to the equations

Positivity of Eigenvectors

- In the computation, we regarding λ as variable and still use $x_1, x_2, \cdots, x_m$ to represent all variables. Let $ps = \{(\mathbf{A} - \lambda\mathbf{E})\mathbf{x}, x_1^2 + \cdots + x_n^2 - 1\}$ and its ideal be I, construct finite-dimensional algebra $QA = R(x_1, x_2, \cdots, x_m)/I$. Clearly, all the polynomial in Q_A is a linear combinarions of the monomials $x^\alpha \notin \langle I \rangle$. Since all of monomials are linearly independent in Q_A, so we called it as S-basis of Q_A.

  In order to obtain S-basis of polynomials, compute Gröbner basis G and assume that $G = \{g_1, g_2, \cdots, g_n\}$.Those monomials not lying in the ideal $\langle LT(I) \rangle$ produce the S-basis of Q_A.

Positivity of Eigenvectors

- Then, we use multiplication to define a linear map m_f from Q_A to itself, where f is any polynomial. Using f multiply with any m_i in Q_A, the result is mapping to Q_A and let it be $fm_i = a_{1i}m_1 + a_{2i}m_2 + \cdots + a_{ki}m_k$. Therefore, for polynomial f there is a matrix

$$m = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{bmatrix}$$

Positivity of Eigenvectors

According to the theory in reference [5], any eigenvalue of m is a value of the function f on $V(I)$. Same with polynomial f, there is a matrix corresponds to each monomial $m_{ij} = m_i \cdot m_j \in A$ respectively, we represent it as m_{ij} still. All traces of matrix m_{ij} constructs an another matrix

$$M = \begin{bmatrix} Tr(m_{11}) & Tr(m_{12}) & \cdots & Tr(m_{1m}) \\ Tr(m_{21}) & Tr(m_{22}) & \cdots & Tr(m_{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ Tr(m_{m1}) & Tr(m_{m2}) & \cdots & Tr(m_{mm}) \end{bmatrix}$$

Positivity of Eigenvectors

Clearly, M is a symmetry matrix. Hence, all of its eigenvalues are real. Moreover, $Tr(m_{ij})$ equals to the sum of m_{ij}'s eigenvalues and it is $\sum_{p \in V(I)} \mu(p) p^{\alpha(i)} p^{\alpha}(j)$, where $p^{\alpha(i)}$ denotes the value of the monomial $x^{\alpha(i)}$ at the point $p \in V(I)$ and $\mu(p)$ is the multiplicity of p.

Similarly, given a polynomial $h \in k[x_1, x_2, \cdots, x_m]$ and $hm_{ij} = hm_i m_j$, there exists a matrix M_h whose i, j entry is the form of $\sum_{p \in V(I)} h(p)\mu(p) p^{\alpha(i)} p^{\alpha(j)}$.

From this, we obtain a matrix factorization $M_h = W \Delta h W^t$, where W is a matrix whose i, j entry is $m_i(p_j)$ and Δh is the diagonal matrix with entries $h(p_1), h(p_2) \cdots h(p_k)$.

Positivity of Eigenvectors

According to linear algebra, there are two fundamental invariants under such changes of basis–the signature $\sigma(hm_{ij})$ and the rank $\rho(hm_{ij})$. There is the following theorem.

Theorem[Ref.[5]]. Let I be a zero-dimensional ideal generated by polynomials in $k[x_1, \cdots, x_n](k \subset R)$, so that $V(I) \subset C^n$ is finite. Then, for $h \in k[x_1, \cdots, x_n]$, the signature and rank of the bilinear form $S_h(f, g) = Tr(m_{hfg})$ satisfy:

$\sigma(S_h) = \#\{a \in V(I) \cap R^n : h(a) > 0\} - \#\{a \in V(I) \cap R^n : h(a) < 0\}$

$\rho(S_h) = \#\{a \in V(I) : h(a) \neq 0\}$.

Positivity of Eigenvectors

- In the decidability of program termination, let $h = \{\mathbf{c^T x}, \lambda\}$, we check whether there exists positive $\mathbf{x}, \boldsymbol{\lambda}$ such that $h(v) > 0$ according to thereom in ref(5).
- Let λ be the eigenvalue of A and $h = C^T x$, now the problem convert to count the number of positive zeros such that $\lambda > 0$ and $h > 0$. If the number is greater than 0, program P is nonterminating.

Positivity of Eigenvectors

- In the verification, we use any constraint condition, say h_k, to multiply any $m_i m_j$ and construct a matrix $m_{hm_{ij}}$. Its trace is the entry (i, j) in M_{h_k}. Next, we get the characteristic polynomial $cp(t)$ of M_{h_k} and count the number of sign changes in the sequence of coefficients of $cp(t)$.
- Let $t = -t$, we count the number of sign changes once again.
- Assume both numbers are n_1 and n_2 respectively, then compute the signature $\sigma(M_h) = n_1 - n_2$ and it is the signature of Δh_k too. According to theorem in ref(5), $n_1 - n_2$ is the difference of number of real zeros such that $h_k > 0$ and number of those such that $h_k < 0$.

Positivity of Eigenvectors

Usually, h is a set of n constraint conditions and those conditions form a "box". We should decide whether there exists positive eigenvector in this box. For this, we count the number of sign changes of $cp(t)$ for any $H||m > 0$ in h, where $H||m$ represents the multiplication of any m constraint conditions. Finally, the number of real zeros that satisfy $h > 0$ is

$$N_R = \frac{1}{2^n} \sum_{i=1}^{m} \sum_{j=1}^{C_n^i} S(H||i_j), m = 1..n \tag{3}$$

Experiment Result

Example

The effect of two sequential assignments $x := x - y; y := x + 2y$ is captured by the simultaneous assignment[1]

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

In the linear program,

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$$

Its characteristic polynomial is $f = t^2 - 3t + 3$ and $f' = 2t - 3$.

Experiment Result

Let $g(t) = 1$, we compute $R(t) = rem(f'g, f) = 2t - 3$. On the base of this, the discriminant matrix is constructed as follows:

$$D = \begin{bmatrix} 1 & -3 & 3 & 0 \\ 0 & 2 & -3 & 0 \\ 0 & 1 & -3 & 3 \\ 0 & 0 & 2 & -3 \end{bmatrix}$$

According to the definition, RSL of D discriminant sequence is $[1, 1, -1]$. So the number of sign change is 1, it means that the number of real eigenvalues is $2 - 2 \times 1 = 0$. So no matter what the loop condition is, this program is terminating always.

Experiment Result

Example

While $(7x + 9y - 10z > 0)\{X := AX\}[4]$, where $X = [x \;\; y \;\; z]^T$ and

$$A = \begin{pmatrix} 7 & -10 & 17 \\ 3 & 9 & 2 \\ -4 & 5 & 13 \end{pmatrix}$$

Construct the equations $(A - \lambda E)X = 0$ in eigenvalues λ.
According to analysis before, add $x^2 + y^2 + z^2 - 1 = 0$ to the system.
Compute the Gröbner basis G in total degree ordering. According to G, those monomials $m_m \notin \langle LT(G) \rangle$ are $Q_A = [1, x, y, z, \lambda, \lambda^2]$.

Experiment Result

Let $h = 1$,

$$M_{h=1} \begin{bmatrix} 6 & 0 & 0 & 0 & 58 & 246 \\ 0 & \frac{7013}{1178} & \frac{1367}{1767} & \frac{1119}{1178} & 0 & 0 \\ 0 & \frac{1367}{1767} & \frac{129}{1178} & \frac{4657}{3534} & 0 & 0 \\ 0 & \frac{1119}{1178} & \frac{4657}{3534} & -\frac{37}{589} & 0 & 0 \\ 58 & 0 & 0 & 0 & 246 & -1172 \\ 246 & 0 & 0 & 0 & -1172 & -1314 \end{bmatrix}$$

Experiment Result

- Its sign characteristic polynomial is $sc = t^6 + t^5 - t^4 + t^3 - t^2 - t + 1$. This indicates that the number of real zeros is $S_1 = 2$. Then, let $h = 7x + 9y - 10z$, we get the number of sign changes is $S_h = 0$. At last, we compute $N_R = \frac{1}{2}(2+0) = 1$ which means there exists a positive eigenvalue and its eigenvector such that $\mathbf{c}^T\mathbf{v} > 0$. Therefore, this linear loop program is nonterminating.
- For the decidability of Example 3 refer to the paper.

Conclusion

- We use discriminant matrix of the characteristic polynomial to construct revised Sturm List so as to know the number of positive eigenvalues. If there is no positive eigenvalue, the linear program is terminating.
- Consideration of the symmetry of Bezout matrix, the signature of characteristic polynomial replaces the sign changes in RSL.

- When the positive eignevalue exists, the termination problem is converted to counting the number of real zeros of polynomial system with constraint conditions by using Gröbner basis. Then, we use signature method to check the existence of real zeros.
- The method in the talk avoids the error of approximate computation and can decide the termination of the program correctly.

Reference

- Tiwari A. *Termination of linear Programs*. CAV'04. 2004, LNCS3114:70-82.
- Yang L, Xia BC.*Automated Proving and Discovery of Inequalities*. Science Press. 2008.
- Yang L, Zhan N, Xia B,et al. *Program verification by Using DISCOVERER*. Proc.VSTTE'05,Zurich. 2005.
- Li J, Li Y, Feng Y. *Termination of a Class of Nonlinear Loop Programs*. Journal of Sichuan University(Engineering Science Edition). 2009,Vol.41(1):129-133.
- David,A.Cox., John, B.Little., Donald, B., O'Shea.*Using Algebric Geometry*, Springer-Verlag New York,Inc(1998).

- Mirshra B. *Algorithmic Algebra*. Springer-Verlag New York, Inc. 1993.
- Bradley AR, Manna Z, Sipma H B. *Termination of Polynomial Programs*. In Proc. VMCAI'05, LNCS3385, Springer Verlag, 2005.
- Yang, L., Zhang, J.Z., and Hou,X.R. *Nonlinear Algebraic Equation System and Automated Theorem Proving.* ShangHai Scientific and Technological Education Publishing House, Shanghai(1996, in Chinese).
- Zhou, CZ. *Formal Techniques for software Embeded System*. Shanghai: East-China Normal University. 2008.

Thank you!