ПРОГРАММНО–
ТЕХНИЧЕСКИЕ
КОМПЛЕКСЫ

М.С. ЛЬВОВ

УДК 004.421.6

МЕТОД ДОКАЗАТЕЛЬСТВА ИНВАРИАНТНОСТИ ЛИНЕЙНЫХ НЕРАВЕНСТВ ДЛЯ ЛИНЕЙНЫХ ЦИКЛОВ

Аннотация. Представлен новый метод доказательства инвариантности системы линейных неравенств для итеративных циклов, определенных над полем рациональных чисел с линейным оператором в теле цикла. Метод учитывает предусловие цикла в виде системы линейных неравенств. Рассмотрения ограничены случаем, когда все собственные значения линейного оператора вещественны. Метод основан на вычислении числа итераций цикла, после выполнения которых инвариантность системы линейных неравенств либо обеспечивается, либо опровергается. Метод использует представление линейного оператора в его жордановой форме.

Ключевые слова: статический анализ программ, линейные инварианты циклов, инвариантные системы линейных неравенств.

ВВЕДЕНИЕ

Проблема поиска инвариантов в контрольных точках императивных программ поставлена в работах Р. Флойда [1] и С. Хоара [2] как ключевая проблема анализа свойств программ. Основное внимание в исследованиях уделялось проблеме построения полиномиальных инвариантов типа равенств. Множество инвариантов типа равенств образует полиномиальный идеал, конечный базис которого нужно построить. В общем случае задача построения такого базиса еще не решена. В [3] предложены общие итеративные методы генерации программных инвариантов, применимые для многих предметных областей. В [4–7] приведен метод доказательства инвариантности полинома и построения базиса векторного пространства полиномиальных инвариантов ограниченной степени. В [8] дано решение задач построения базиса векторного пространства полиномиальных инвариантов для класса программ с процедурами, все вычисления в которой линейны. Многие работы, например [9–13], посвящены более частной, но ключевой задаче построения инвариантных равенств для итеративных циклов. В частности, в [11–13] исследуется задача построения базиса идеала полиномиальных инвариантных равенств для линейных циклов.

Задача описания инвариантных неравенств менее изучена. Основная сложность здесь — бесконечность базиса метаидеала полиномиальных неравенств [12, 13]. Итеративные методы решения задачи описания линейных инвариантных неравенств рассматривалась в [14–17]. В [14] решена задача генерации простейших инвариантных неравенств. В [15, 16] к задаче поиска линейных инвариантных неравенств применяются общие итеративные методы.

Математические определения и результаты, используемые в настоящей работе, можно найти, например, в [19, 20].

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Определение 1. Пусть Q^n — n-мерное векторное пространство над полем рациональных чисел Q и $\overline{Q}$ — алгебраическое замыкание поля Q.

Определение 2. Пусть $X = (x_1, ..., x_n)$, $b = (b_1, ..., b_n)$ — два вектора переменных. Линейным циклом с предусловием называется фрагмент императивной программы вида

$$X := b;\ //\ S(b)\ —\ \text{предусловие}$$

$$\textbf{While}\ U(X, b)\ \textbf{do}\ X := A * X. \tag{1}$$

Здесь вектор b удовлетворяет системе линейных неравенств с рациональными коэффициентами $S(b)$, $U(X, b)$ — бесквантерная формула прикладной логики линейных полуалгебраических множеств, A — матрица линейного оператора $Q^n \to Q^n$.

Замечание 1. Операторы $X := b$, $X := A * X$ интерпретируются как одновременные присвоения переменным левых частей значений правых частей.

Определение 3. Линейное неравенство $P(X, b) \in Q^1[X, b]$ называется инвариантным для цикла (1) с предусловием $S(b)$, если оно выполняется всякий раз в результате выполнения тела цикла: $P(X, b) \overset{df}{=} a_1x_1 + ... + a_nx_n < a'_1b_1 + ... + a'_nb_n$. Таким образом, инвариантность означает выполнение последовательности формул:

$S(b) \to P(b, b)$, // инвариант выполняется при входе в цикл,

$U(b, b) \to P(Ab, b)$, // инвариант выполняется после 1-й итерации,

$U(Ab, b) \to P(A^2b, b)$, // инвариант выполняется после 2-й итерации,

...

$U(A^kb, b) \to P(A^{k+1}b, b)$, // инвариант выполняется после k-й итерации,

$\neg U(A^kb, b) \to P(A^kb, b)$, // инвариант выполняется при завершении цикла.

Теорема 1. Если все собственные значения $\Lambda = (\lambda_1, ..., \lambda_n)$, $\lambda_i \in \overline{Q}$ оператора A вещественны, проблема доказательства инвариантности $P(X, b)$ для цикла (1) алгоритмически разрешима.

Доказательство. Доказательство инвариантности системы линейных неравенств очевидным образом сводится к доказательству инвариантности каждого из неравенств системы. Поэтому в леммах 1–5 изложен метод доказательства инвариантности линейного неравенства.

Рассмотрим линейное неравенство с рациональными коэффициентами

$$a_1x_1 + a_2x_2 + ... + a_nx_n \le c,\ c = c(b). \tag{2}$$

Задача состоит в том, чтобы доказать или опровергнуть инвариантность этого неравенства для цикла (1). Предположим сначала, что линейный оператор в теле цикла диагонализируем. В базисе собственных векторов его матрица и ее m-я степень будут иметь вид

$$A = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix},\ A^m = \begin{bmatrix} \lambda_1^m & 0 & \dots & 0 \\ 0 & \lambda_2^m & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n^m \end{bmatrix}.$$

Замечание 2. После перехода к базису из собственных векторов коэффициенты неравенства изменятся. Если $S(\Lambda)$ — матрица перехода, то новые значения векторов a, b вычисляются по формулам $a^{(S)} = SaS^{-1}$, $b^{(S)} = SbS^{-1}$. Чтобы не перегружать текст новыми обозначениями, используем старые.

Рассмотрим сначала абсолютно недетерминированный цикл

$X := b;\ //\ S(b)$ — предусловие,

$\textbf{While}\ \text{True} \mid \text{False}\ \textbf{do}\ X := A * X.$ (3)

Лемма 1. Утверждение теоремы справедливо для цикла (3) при $S(b)=\{b\}$.

Доказательство. Пусть b — произвольный вектор из Q^n. Предположим, что $S(b)=\{b\}$. Перед входом в цикл инвариантность (2) означает, что

$$a_1b_1+a_2b_2+\ldots+a_nb_n\le c. \tag{4}$$

После m итераций цикла инвариантность (2) означает, что

$$\lambda_1^m a_1b_1+\lambda_2^m a_2b_2+\ldots+\lambda_n^m a_nb_n\le c. \tag{5}$$

Без ограничения общности можно считать, что $|\lambda_1|>\max(|\lambda_2|,\ldots,|\lambda_n|)$, а также $a_1\ne 0, b_1\ne 0$, поскольку в противном случае переменная x_1 в вычислениях не участвует. Рассмотрим различные случаи.

1. Пусть $|\lambda_1|\le 1$. Отображение $A:Q^n\to Q^n$ сжимающее.

1.1. Если $\lambda_1>0$, неравенство (4) перепишем в виде

$$a_1b_1+(\lambda_2^m/\lambda_1^m)a_2b_2+\ldots+(\lambda_n^m/\lambda_1^m)a_nb_n\le c/\lambda_1^m. \tag{6}$$

Поскольку $\lambda_j^m/\lambda_1^m\underset{m\to\infty}{\to}0$, $c/\lambda_1^m\underset{m\to\infty}{\to}\infty$, при $c>0$ существует такое натуральное M_0, что при $m>M_0$ (5) выполняется. При $c<0$ существует такое натуральное M_0, что при $m>M_0$ (6) ложно. Следовательно, в обоих случаях инвариантность (2) можно установить конечным числом $m\le M_0$ проверок.

1.2. Если $\lambda_1<0$, неравенство (6) перепишем в виде системы неравенств — четном и нечетном числе повторений цикла

$$\begin{gathered}a_1b_1+(\lambda_2^{2m}/\lambda_1^{2m})a_2b_2+\ldots+(\lambda_n^{2m}/\lambda_1^{2m})a_nb_n\le c/\lambda_1^{2m},\\ a_1b_1+(\lambda_2^{2m+1}/\lambda_1^{2m+1})a_2b_2+\ldots+(\lambda_n^{2m+1}/\lambda_1^{2m+1})a_nb_n\ge c/\lambda_1^{2m+1}.\end{gathered} \tag{7}$$

При $c>0$ существует такое натуральное M_0, что при $m>M_0$ система (7) выполняется. Следовательно, в этом случае инвариантность (2) можно установить конечным числом $m\le M_0$ проверок. При $c<0$ система (7) ложна.

2. Будем считать, что $|\lambda_1|>1$. Как и в п. 1, рассмотрим несколько случаев.

2.1. Пусть $\lambda_1>0$. Приведем неравенство (5) к виду

$$a_1b_1+(\lambda_2^m/\lambda_1^m)a_2b_2+\ldots+(\lambda_n^m/\lambda_1^m)a_nb_n\le(c/\lambda_1^m). \tag{8}$$

Далее,

$$a_1b_1\le(c/\lambda_1^m)-(\lambda_2^m/\lambda_1^m)a_2b_2-\ldots-(\lambda_n^m/\lambda_1^m)a_nb_n. \tag{9}$$

Поскольку $|\lambda_j/\lambda_1|<1$ и $|\lambda_1|>1$, $\lambda_j^m/\lambda_1^m\underset{m\to\infty}{\to}0$, $c/\lambda_1^m\underset{m\to\infty}{\to}0$, при достаточно больших значениях m и каждое слагаемое правой части, и модуль правой части неравенства могут быть сколь угодно малыми:

$$|(c/\lambda_1^m)-(\lambda_2^m/\lambda_1^m)a_2b_2-\ldots-(\lambda_n^m/\lambda_1^m)a_nb_n|<\varepsilon.$$

Таким образом, при $m>M_0(\varepsilon)$ имеем

$$|a_1b_1|\le\varepsilon. \tag{10}$$

2.1а. Следовательно, если $a_1b_1>0$, ε можно выбрать настолько малым, что $a_1b_1>\varepsilon>0$. Это противоречит (6). Значит, неравенство (2) не является инвариантным, поскольку оно не выполняется при $m>M_0(\varepsilon)$.

2.1б. Если же $a_1b_1<0$, неравенство (2) выполняется при всех $m>M_0(\varepsilon)$. Таким образом, инвариантность (2) может быть установлена проверками конечного числа M соотношений, определяющих инвариантность неравенства из определения 3.

3. Рассмотрим случай $\lambda_1<0$. Как и в п. 1.2б, при четных m имеет место неравенство (6), при нечетных m — неравенство

$$a_1b_1\ge(c/\lambda_1^m)-(\lambda_2^m/\lambda_1^m)a_2b_2-\ldots-(\lambda_n^m/\lambda_1^m)a_nb_n,$$

т.е. $a_1 b_1 \geq \varepsilon$. Поскольку в цикле четные и нечетные значения m чередуются, (2) не является инвариантом.

Лемма 2. Утверждение теоремы справедливо для цикла (3) при $S(b) = BoundPolygon(b^{(1)}, ..., b^{(k)})$.

Доказательство. Рассмотрим случай, когда $S(b)$ — ограниченная многогранная область Q^n, натянутая на векторы $b^{(1)}, ..., b^{(k)}$. В этом случае произвольный вектор из $S(b)$ можно представить в виде

$$b = \alpha_1 b^{(1)} + ... + \alpha_k b^{(k)},\ \alpha_j \geq 0,\ \alpha_1 + ... + \alpha_k = 1.$$

Тогда случай 2.1б должен иметь место для каждого $b(j)$, $j = 1, ..., k$: при $m_j > M_{0j}(\varepsilon)$ выполняется $a_1 b_1^{(j)} < 0$. При этом из $b = \alpha_1 b^{(1)} + ... + \alpha_k b^{(k)}$ следует, что $b_1 = \alpha_1 b_1^{(1)} + ... + \alpha_k b_1^{(k)}$ и при $m > \max [M_{01}(\varepsilon), ..., M_{0k}(\varepsilon)]$ имеет место $a_1 b_1 < 0$.

Лемма 3. Утверждение теоремы справедливо для цикла (3) при $S(b) = UnboundPolygon(b^{(1)}, \ldots, b^{(k)})$.

Доказательство. Предположим, что область $S(b)$ не ограничена. Вычислим $Max = \max (P(x, b), X \in S(b))$. Этот максимум либо конечен и достигается в одной из вершин $S(b)$, либо бесконечен. Вычисление Max осуществляется методами линейного программирования. Для инвариантности (4) необходимо, чтобы $Max < c$ при вычислениях, приведенных в лемме 2.

Для полноты доказательства в случае диагонализируемой матрицы оператора A осталось рассмотреть случай, когда несколько модулей собственных значений принимают максимальные значения:

$$|\lambda_1| = ... = |\lambda_k| > \max (|\lambda_{k+1}|, \ldots, |\lambda_n|).$$

Неравенство (5) имеет вид $a_1 b_1 + ... + a_k d_k \leq \varepsilon$, и все рассуждения остаются прежними.

Лемма 4. Утверждение теоремы цикла (3) справедливо в случае, когда оператор A в жордановой форме имеет нетривиальные жордановы клетки.

Доказательство. Пусть матрица оператора A в жордановой форме имеет нетривиальные жордановы клетки. Напомним, что жордановой клеткой называется $n \times n$-матрица

$$J(\lambda) = \begin{bmatrix} \lambda & 1 & \ldots & 0 \\ 0 & \lambda & \ldots & 0 \\ 0 & \ldots & \lambda & 1 \\ 0 & \ldots & 0 & \lambda \end{bmatrix} \tag{11}$$

и матрица оператора A имеет вид $A = J_1(\lambda_1) \times ... \times J_l(\lambda_l)$, т.е. составлена из нескольких жордановых клеток, раположенных по главной диагонали, причем каждая жорданова клетка определяется своим собственным значением оператора A. Каждой клетке $J_j(\lambda_i)$ соответствует своя группа переменных. Поэтому доказательство достаточно провести только для одной клетки размера k, обозначенной в (11). Пусть $X = (x_1, ..., x_k)$, m — натуральное число и $b = (b_1, ..., b_k)$ — вектор переменных (начальних значений). Вычислив m-ю итерацию $X^{(0)} = b$; $X^{(m)} = AX^{(m)}$ в явном виде $X^{(m)} = A^m X$: $X^{(m)} = J(\lambda)^m b$, получим

$$X^{(m)} = \begin{bmatrix} \lambda^m & C_1(m) & \ldots & C_{k-1}(m) \\ 0 & \lambda^m & \ldots & C_{k-2}(m) \\ 0 & \ldots & \lambda^m & C_1(m) \\ 0 & \ldots & 0 & \lambda^m \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \ldots \\ b_k \end{bmatrix}, \tag{12}$$

где $C_j(m) = C_m^j \lambda^{m-j} = \dfrac{m(m-1)\ldots(m-j+1)}{j!} \lambda^{m-j}$, $j \in 1 \ldots k-1$.

Рассмотрим равенство, соответствующее j-й строке матричного равенства

$$x_j^{(m)} = \lambda^m \left(b_j + \frac{C_1(m)}{\lambda} b_{j+1} + \ldots + \frac{C_{k-j}(m)}{\lambda^{k-j}} b_k \right) \stackrel{df}{=} \lambda^m g_j(m, \lambda, b). \qquad (13)$$

Левая часть неравенства (5) представляет собой сумму, каждое слагаемое которой определено группой переменных клетки $J_j(\lambda_i)$:

$$\lambda_j^m S_j^{(m)} = \lambda_j^m (g_1(m, \lambda_j, b_{j1}) a_{j1} + g_2(m, \lambda_j, b_{j2}) a_{j2} + \ldots + g(m, \lambda_j, b_{jk_j}) a_{jk_j}). \qquad (14)$$

Аналог неравенства (5) имеет вид

$$\lambda_1^m S_1^{(m)} + \lambda_2^m S_2^{(m)} + \ldots + \lambda_l^m S_l^{(m)} \le c. \qquad (15)$$

Пусть λ_1 — максимальное значение: $|\lambda_1| = \max(|\lambda_1|, \ldots, |\lambda_l|)$. Тогда, поскольку $S_j^{(m)}$ — многочлен от m, а $(\lambda_j / \lambda_1)^m$ — показательная функция от m и $\lambda_j / \lambda_1 > 1$, имеем

$$\frac{\lambda_j^m S_j^{(m)}}{\lambda_1^m} \underset{m \to \infty}{\to} 0 \text{ при } \lambda_j \ne \lambda_1.$$

Поэтому метод, описанный в леммах 1–3, можно использовать и для (9) , т.е. в общем случае. Не повторяя рассмотрение всех случаев леммы 1, ограничимся случаем $\lambda_1 > 1$. Как и в лемме 1, необходимое условие существования инварианта $S_1^{(m)} < 0$ запишем

$$S_1^{(m)} = g_1(m, \lambda_1, b_{11}) a_{11} + g_2(m, \lambda_1, b_{21}) a_{12} + \ldots + g(m, \lambda_1, b_{1k_1}) a_{1k_1},$$

$S_1^{(m)}$ — многочлен от переменной m. Для того чтобы обеспечить неравенство $S_1^{(m)} < 0$ при всех $m > M_0$, необходимо, чтобы коэффициент $Lc(S_1^{(m)})$ при старшей степени $S_1^{(m)}$ был меньше нуля. Из (12), (13) следует, что $Lc(S_1^{(m)}) = Lc(C_{k_1}(m) a_{1k_1} b_{1k_1})$, но $Lc(C_{k_1}(m) = m^{k_1} / \lambda_1^{k_1} > 0$. Поэтому $a_{1k_1} b_{1k_1} < 0$ — необходимое условие инвариантности неравенства. Для цикла (3) теорема доказана.

Лемма 5. Утверждение теоремы справедливо для цикла (1) (рис. 1).

Доказательство. Анализ цикла (1), иллюстрированный блок-схемой рис. 1, показывает, что образ мнообразия $S(b)$ после m-кратного выполнения цикла в контрольной точке C_1 описывается системой неравенств $s(A^m b) \& U(A^m b, b)$. Следовательно, метод лемм 1–4, применяемый к предусловию $s(b) \& U(b, b)$, решает задачу доказательства инвариантности неравенства в контрольной точке C_1. Таким образом, существует такое натуральное число M_0, что если количество m повторений цикла превосходит M_0 и $U(X, b)$ выполняется для $k = 0, 1, \ldots, M_0$, то $U(X, b)$ выполняется при любом $m > M_0$.

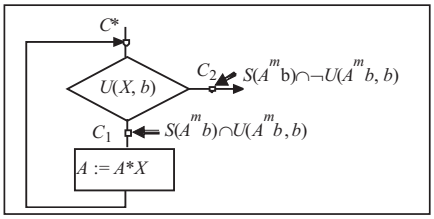

Рис. 1. Схема цикла (1) и инварианты его контрольных точек

Теорема доказана.

ЗАКЛЮЧЕНИЕ

В настоящей работе представлена только основная идея метода. Алгоритмы компьютерной алгебры, связанные, например, с вычислениями матрицы перехода к базису собственных векторов $S(\Lambda)$, построением жордановой формы A, вычислением $a^{(S)} = SaS^{-1}, b^{(S)} = SbS^{-1}$, оценками числа m итераций метода,

алгоритмами отделения и уточнения корней $\Lambda = (\lambda_1, ..., \lambda_n), \lambda_i \in \overline{Q}$, характеристического многочлена, проверки инвариантности первых m сотношений в определении (3), здесь не обсуждаются. Их можно найти в [20].

Реально предположить, что метод может применяться и к произвольным операторам A (с комплексными собственными значениями), а также служить основой общего алгоритма доказательства инвариантности системы линейных неравенств для линейно-определенных программ, аналогичного методу доказательства инвариантности полиномиальных равенств [5, 6].

СПИСОК ЛИТЕРАТУРЫ

1. Floyd R.W. Assigning meanings to programs // Proc. of Symp. on Appl. Math. / J.T. Schwartz (Ed.). — Providence (R.I.): Amer. Math. Soc. — 1967. — **19**. — P. 19–32.
2. Hoare C.A.R. An axiomatic basis for computer programming // Communic. ACM. — New York: ACM, 1969. — N 12(10). — P. 576–580.
3. Godlevsky A.B., Kapitonova Y.V., Krivoy S.L., Letichevsky A.A. Iterative methods of program analysis // Cybernetics. — 1989. — N 2. — P. 9–19.
4. Львов М.С. Инвариантные равенства малых степеней в программах, определенных над полем // Кибернетика. — 1988. — № 1. — С. 108–110.
5. Letichevsky A., Lvov M. Discovery of invariant equalities in programs over data fields // Appl. Algebra in Eng., Com. and Comput. — 1993. — N 4. — P. 21–29.
6. Lvov M. About one algorithm of program polynomial invariants generation / M. Giese, T. Jebelean (Eds.) // Proc. Workshop on Invariant Generation, WING 2007. Techn. Rep. N 07-07 in RISC Report Series, University of Linz, Austria. 06 2007. Workshop Proceedings. — P. 85–99 (electronic).
7. Müller-Olm M., Seidl H. Computing polynomial program invariants // Inf. Process. Lett. — 2004. — **91**, N 5. — P. 233–244.
8. Müller-Olm M., Seidl H. Precise interprocedural analisys through linear algebra // Proc. of the 31st ACM SIGPLAN-SIGACT Symp. on Principles of Program. Languages. SIGPLAN Notices — POPL'04. — 2004. — **39**, N 1. — P. 330–341.
9. Sankaranarayanan S., Sipma H., Manna Z. Non-linear loop invariant generation using Gröbner bases // Proc. of Symp. on Principles of Program. Languages. — Venice, Italy, January 14–16, 2004. — New York: ACM, 2004. — P. 318–329.
10. Rodriguez-Carbonell E., Kapur D. Automatic generation of polynomial loop invariants: algebraic foundations // Proc. of Intern. Symp. on Symbolic and Algebraic Comp. — Santander, Spain, July 4–7, 2004. — New York: ACM, 2004. — P. 266–273.
11. Kovács L.I., Jebelean T. An algorithm for automated generation of invariants for loops with conditionals // Proc. of Intern. Symp. on Symbolic and Numeric Algorithms for Sci. Comp. — Timisoara, Romania, 2–29 Sept. 2005. IEEE Comput. Soc., 2005. — P. 245–249.
12. Lvov M.S. Polynomial invariants for linear loops // Cybernetics and Systems Analysis. — 2010. — **46**, N 4. — P. 660–668.
13. Львов М.С., Крекнин В.А. Нелинейные инварианты линейных циклов и собственные полиномы линейных операторов // Кибернетика и системный анализ. — 2012. — № 2. — С. 126–139.
14. Cousot P., Halbwachs N. Automatic discovery of linear restraints among variables of a program // Conf. Record of the Fifth Annual ACM SIGPLAN-SIGACT Symp. on Principles of Program. Languages, Tucson, Arizona, 1978. — New York: ACM Press. — P. 84–97.
15. Кривой С.Л., Ракша С.Г. Поиск инвариантных линейных зависимостей в программах // Кибернетика. — 1984. — № 6. — С. 23–28.
16. Годлевский А.В., Капитонова Ю.В., Кривой С.Л., Летичевский А.А. Итеративные методы анализа программ. Равенства и неравенства // Там же. — 1990. — № 3. — С. 1–10.
17. Львов М.С. Инвариантные неравенства в программах, интерпретированных над упорядоченными полями // Там же. — 1986. — № 5. — С. 22–27.
18. Львов М.С. Об инвариантных неравенствах для состояний схем программ, интерпретированных над векторным пространством // Там же. — 1985. — № 2. — С. 111–112.
19. Ван дер Варден Б.Л. Алгебра. — Изд. 2-е. — М.: ГРФМЛ, 1979. — 624 с.
20. Ходж В., Пидо Д. Методы алгебраической геометрии. Т. 1. — М.: Изд-во иностр. лит., 1954. — 462 с.
21. Компьютерная алгебра: символьные и алгебраические вычисления / Под ред. Б. Бухбергера, Дж. Коллинза, Р. Лооса. — М.: Мир, 1986. — 392 с.

Поступила 02.07.2013