ПРОГРАММНО-
ТЕХНИЧЕСКИЕ
КОМПЛЕКСЫ

М.С. ЛЬВОВ

УДК 004.421.6

АНАЛИЗ ЛИНЕЙНО ОПРЕДЕЛЕННЫХ ИТЕРАТИВНЫХ ЦИКЛОВ

Аннотация. Представлен новый метод доказательства инвариантности системы линейных неравенств, а также завершаемости линейно определенных итеративных циклов императивных программ. Тело цикла — линейный оператор, преобразующий вектор переменных программы. Метод учитывает предусловие цикла, а также условие повторения цикла в виде совокупности систем линейных неравенств. Метод основан на построении и анализе спектра этого оператора и вычислении числа итераций цикла, после выполнения которых инвариантность либо обеспечивается, либо опровергается. Теоретический материал работы иллюстрируется примерами.

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

ВВЕДЕНИЕ

Проблема доказательства правильности компьютерных программ была поставлена в основополагающих работах Р. Флойда [1] и Ч. Хоара [2]. Свойство правильности программы формулируют в терминах ее тотальной (полной) корректности (правильности).

Программа P называется тотально корректной, если на ее входе X в результате выполнения предусловия $\varphi(X)$ она завершает свою работу и на выходе $P(X)$ выполнено постусловие $\phi(P(X))$. Программа называется частично корректной, если из предположения $\varphi(X)$ и завершения P следует $\phi(P(X))$.

Доказательство завершаемости программы часто необходимо осуществлять независимо от доказательства ее частичной корректности. Алгоритмическая неразрешимость проблемы остановки означает, что общего алгоритма доказательства завершаемости программы не существует.

Для доказательства частичной корректности программ Р. Флойд и Ч. Хоар предложили идею построения инвариантов циклов [1] и инвариантных соотношений в контрольных точках программ [2], что позволяет доказывать корректность программы методом математической индукции. Таким образом, возникла проблема поиска программных инвариантов как ключевая проблема анализа свойств программ.

Основное внимание в настоящее время уделяется задаче построения полиномиальных инвариантов типа равенств. Множество инвариантов типа равенств образует полиномиальный идеал, конечный базис которого следует построить. В общем случае задача построения такого базиса еще не решена. В [3] предложены общие итеративные методы генерации программных инвариантов, применяемые 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 доказательства инвариантности неравенств менее изучена. Основная сложность здесь — бесконечность базиса метаидеала [20] 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. В [19] изложен метод доказательства инвариантности системы линейных неравенств для класса линейных итеративных циклов с действительными собственными числами линейного оператора в теле цикла. В настоящей работе этот метод распространяется на весь класс линейных итеративных циклов и применяется для доказательства их завершаемости.

Математические определения, результаты и алгоритмы компьютерной алгебры, используемые в статье, можно найти, например, в [20–23].

ПОСТАНОВКА ЗАДАЧИ

Пусть K^n — n-мерное векторное пространство над линейно упорядоченным конструктивным полем K и $\overline{K}$ — алгебраическое замыкание поля K.

Определение 1. Линейным полуалгебраическим множеством $M(x_1,\dots,x_n)$ называется область K^n, определяемая бесквантормой формулой в сигнатуре логических связок $\vee, \&, \neg$ с линейными неравенствами от переменных $x_1,\dots,x_n$ в качестве атомов. Если область M задается формулой $F(X)$, т.е. $M=\{X:F(X)\}$, будем обозначать ее $M(F(X))$.

Определение 2. Пусть $X=(x_1,\dots,x_n)$, $\overline{b}=(b_1,\dots,b_n)$ — векторы переменных. Линейно определенным циклом с предусловием называется фрагмент императивной программы вида

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

While $U(X,$ **b**$)$ **do** X : = A * X, (1)

где $S(\overline{b})$, $U(X,\overline{b})$ — бесквантормые формулы прикладной логики линейных полуалгебраических множеств, A — матрица линейного оператора $K^n \to K^n$.

Нетерминированным циклом, ассоциированным с циклом (1), называется цикл вида

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

While True | False **do** X : = A * X, (2)

количество повторений которого недетерминировано.

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

Определение 3. Последовательность $\{\overline{b}^{(m)}\}$, определенная рекурсивными соотношениями

$$\overline{b}^{(0)}=\overline{b},\ \overline{b}^{(m+1)}=A\overline{b}^{(m)},\ m=0,1,\dots, \tag{3}$$

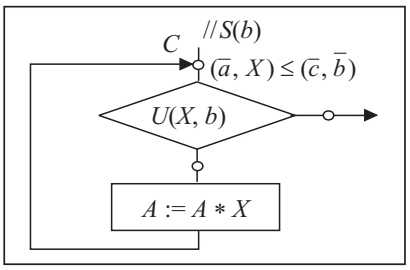

Рис. 1. Схема линейно определенного цикла с контрольной точкой C, в которой определен инвариант

называется орбитой линейного оператора A с начальной точкой $\bar{b}$ и обозначается $Orbit(A, \bar{b})$.

Определение 4. Линейно определенный цикл (1) называется завершаемым, если для любого $\bar{b} \in M(S(X))$ последовательность (3) при некотором натуральном $m^* = m^*(\bar{b})$ удовлетворяет соотношению $\neg U(\bar{b}^{(m^*)}, \bar{b})$.

Таким образом, если цикл завершаем, для каждого $\bar{b} \in M(S(X))$ сушествует наименьшее натуральное число $m^*(\bar{b})$, на котором цикл (1) завершается.

Определение 5. Пусть $\bar{a}, \bar{c} \in K^n$. Линейное неравенство

$$L(\bar{a}, \bar{c}, X, \bar{b}) \overset{df}{=} (\bar{a}, X) \le (\bar{c}, \bar{b}) \tag{4}$$

называется условным инвариантом линейно определенного цикла (1) (с предусловием $S(\bar{b})$), если для любого $\bar{b} \in M(S(X))$ $Orbit(A, \bar{b})$ (см. (3)) удовлетворяет соотношениям

$$S(\bar{b}) \to L(\bar{a}, \bar{c}, \bar{b}, \bar{b}),$$

$$U(\bar{b}^{(m-1)}, \bar{b}) \to L(\bar{a}, \bar{c}, \bar{b}^{(m)}, \bar{b}), \ m = 1, 2, \ldots, m^*(\bar{b}).$$

Замечание 2. Если цикл (1) не завершается (расходится) в некоторой точке $\bar{b}$, то $m^*(\bar{b})$ следует считать равным бесконечности: $m^*(\bar{b}) = +\infty$.

Пример 1. Пусть

$$S(x, y) = (0 \le x \le 1) \,\&\, (0 \le y \le 1),$$

$$U(x, y, b_1, b_2) = \neg(|x + b_1| \le \varepsilon) \,\&\, (|y + b_2| \le \varepsilon),$$

$$A = \begin{bmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{bmatrix},$$

$$L = x + y \le 2b_1 + 2b_2 \ // \ \bar{a} = (1, 1), \ \bar{c} = (2, 2).$$

В этом примере линейный оператор A — оператор поворота на угол $\alpha = \operatorname{arctg}(4/3)$. Начальная точка $\bar{b}$ принадлежит единичному квадрату. Орбита линейного оператора A — последовательность, каждая точка которой лежит на окружности $x^2 + y^2 = b_1^2 + b_2^2$. Условие повторения цикла: точка (x, y) лежит вне квадрата со стороной 2ε и центром в точке $(-b_1, -b_2)$. Поэтому цикл завершится, когда точка попадет внутрь этого квадрата, т.е. совершит поворот на угол $\pi + 2k\pi$ с точностью ε. Поскольку угол α несоизмерим с π, орбита оператора A представляет всюду плотное множество на окружности $x^2 + y^2 = b_1^2 + b_2^2$; сле-

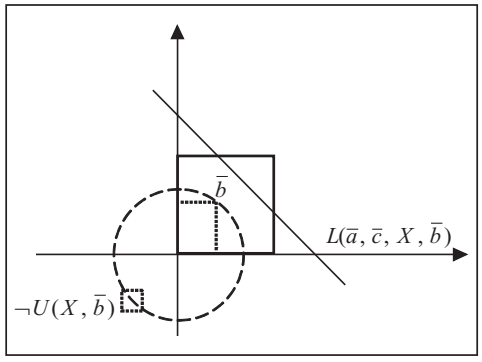

Рис. 2. Геометрическая иллюстрация линейно определенного цикла

довательно, цикл завершится. Ниже основной алгоритм будет применяться для доказательства того, что $L = x + y \le 2b_1 + 2b_2$ — это условный инвариант цикла.

В настоящей работе показано, что проблемы завершаемости цикла (1) и доказательства инвариантности линейного неравенства алгоритмически разрешимы для любого линейного определенного цикла (1).

ПРЕДСТАВЛЕНИЕ ЛИНЕЙНОГО НЕРАВЕНСТВА

Жордановой клеткой называется $m \times m$ матрица вида

$$J(\lambda) = \begin{bmatrix} \lambda & 1 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & \lambda & 1 \\ 0 & \dots & 0 & \lambda \end{bmatrix}. \tag{5}$$

Матрица оператора A в жордановой форме имеет вид

$$A = \begin{bmatrix} J_1(\lambda_1) & 0 & \dots & 0 \\ 0 & J_2(\lambda_2) & \dots & 0 \\ 0 & \dots & J_{k-1}(\lambda_{k-1}) & 0 \\ 0 & \dots & 0 & J_k(\lambda_k) \end{bmatrix},$$

т.е. она составлена из нескольких жордановых клеток различных размеров, расположенных по главной диагонали, причем каждая жорданова клетка определяется своим собственным значением λ_j оператора A. В частности, если линейный оператор в теле цикла (1) диагонализируем, в базисе собственных векторов его матрица имеет вид

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

Пусть $f(x)$ — минимальный характеристический многочлен оператора A; $\Lambda = \{\lambda_1, \dots, \lambda_n\}$ — множество его корней (спектр A); $\bar{e}_1, \dots, \bar{e}_n$ — множество собственных векторов A; $\lambda_1, \dots, \lambda_{2k}$ — множество комплексных собственных чисел, а $\lambda_{2k+1}, \dots, \lambda_n$ — множество действительных собственных чисел, причем $\lambda_1 = \bar{\lambda}_2, \dots, \lambda_{2k-1} = \bar{\lambda}_{2k}$. Определим векторы

$$\bar{l}_1 = \frac{1}{2}(\bar{e}_1 + \bar{e}_2), \quad \bar{l}_2 = \frac{1}{2i}(\bar{e}_1 + \bar{e}_2).$$

В базисе $(\bar{l}_1, \bar{l}_2)$ матрица $A_1 = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \bar{\lambda}_1 \end{bmatrix}$ имеет вид $B_1 = \begin{bmatrix} \alpha_1 & \beta_1 \\ -\beta_1 & \alpha_1 \end{bmatrix}$, где $\lambda_1 = \alpha_1 + i\beta_1$, $\lambda_2 = \alpha_1 - i\beta_1$. Применив такое преобразование ко всем парам собственных векторов с попарно сопряженными комплексными собственными числами, получим представление линейного оператора в так называемой вещественной жордановой форме

$$A'=\begin{bmatrix} B_1 & 0 & . & 0 & . & . & 0 \\ 0 & B_2 & . & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & \dots & 0 & B_k & . & \dots & 0 \\ 0 & . & . & 0 & \lambda_{2k+1} & \dots & 0 \\ . & . & . & . & . & . & . \\ 0 & . & . & . & 0 & \dots & \lambda_n \end{bmatrix}.$$

Замечание 3. После перехода к базису из собственных векторов коэффициенты неравенства изменятся. Если $S(\Lambda)$ — матрица перехода, то новые значения векторов $\bar{a}, \bar{b}$ вычисляются по формулам $\bar{a}^{(S)} = S\bar{a}S^{-1}$, $\bar{b}^{(S)} = S\bar{b}S^{-1}$. Чтобы не перегружать текст новыми обозначениями, будем применять обозначения, используемые ранее.

Заметим, что матрица вида $\hat{B} \overset{df}{=} \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}$, где $\alpha^2 + \beta^2 = 1$ является матрицей поворота вектора 2-мерного пространства на угол φ, определенный соотношениями $\cos(\varphi) = \alpha$, $\sin(\varphi) = \beta$. Поэтому

$$B_1 = r_1 \begin{bmatrix} \cos(\varphi_1) & \sin(\varphi_1) \\ -\sin(\varphi_1) & \cos(\varphi_1) \end{bmatrix}, \; r_1 = |\lambda_1| = \sqrt{\alpha^2 + \beta^2}.$$

Неравенство (4), инвариантность которого рассматривается для цикла (2) с конкретным начальным значением $\bar{b}$, означает $\forall X \in Orbit(A, \bar{b})(\bar{a}, X) \le (\bar{c}, \bar{b})$. Алгоритм доказательства инвариантности (4) будем формулировать в эквивалентном виде: $\underset{X \in Orbit(A, \bar{b})}{\mathrm{Sup}} (\bar{a}, X) \le (\bar{c}, \bar{b})$.

Рассмотрим линейную форму $a_1x_1 + a_2x_2 + \dots + a_nx_n \overset{df}{=} (\bar{a}, X)$. Преобразование $X := A * X$ переводит эту форму в (a, AX), а m-кратная итерация цикла, описываемая преобразованием $X := A^m * X$, — переводит в $(a, A^m X)$.

Пусть $X_1 = (x_1, x_2), \dots, X_k = (x_{2k-1}, x_{2k})$, $\bar{a}_1 = (a_1, a_2), \dots, \bar{a}_k = (a_{2k-1}, a_{2k})$. Тогда

$$(\bar{a}, X) = (\bar{a}_1, X_1) + \dots + (\bar{a}_k, X_k) + a_{2k+1}x_{2k+1} + \dots + a_nx_n. \qquad (6)$$

Преобразование $(\bar{a}, AX)$ линейной формы может быть записано в виде

$$(\bar{a}, AX) = (\bar{a}_1, B_1X_1) + \dots + (\bar{a}_k, B_kX_k) + \lambda_{2k+1}a_{2k+1}x_{2k+1} + \dots + \lambda_n a_n x_n, \qquad (7)$$

а его m-я итерация — в виде

$$(\bar{a}, A^mX) = (\bar{a}_1, B_1^mX_1) + \dots + (\bar{a}_k, B_k^mX_k) + \lambda_{2k+1}^m a_{2k+1}x_{2k+1} + \dots + \lambda_n^m a_n x_n. \qquad (8)$$

Перейдя в (8) к представлению в виде $B_j = r_j\hat{B}_j$, получим

$$(\bar{a}, A^mX) = r_1^m(\bar{a}_1, \hat{B}_1^mX_1) + \dots + r_k^m(\bar{a}_k, \hat{B}_k^mX_k) + \lambda_{2k+1}^m a_{2k+1}x_{2k+1} + \dots + \lambda_n^m a_n x_n .$$

МЕТОД ПРОВЕРКИ ИНВАРИАНТНОСТИ НЕРАВЕНСТВА ДЛЯ ДИАГОНАЛИЗИРУЕМОГО ЛИНЕЙНОГО ОПЕРАТОРА

Рассмотрим вопрос о множестве значений орбиты оператора $(\bar{a}_1, \hat{B}_1^m X_1) + \dots + (\bar{a}_k, \hat{B}_k^m X_k)$ для начального значения $\bar{b}^{(0)} = (\bar{b}_1^{(0)}, \dots, \bar{b}_k^{(0)})$, где $\bar{b}_j = (b_{2j-1}, b_{2j})$, $j = 1, \dots, k$. Будем интерпретировать пары X_j, как точки на

2-мерной плоскости, а преобразования $\hat{B}_j \overset{df}{=} \begin{bmatrix} \cos(\varphi_j) & \sin(\varphi_j) \\ -\sin(\varphi_j) & \cos(\varphi_j) \end{bmatrix}$ — как повороты точек X_j на угол φ_j.

Лемма 1. Пусть

$$B(\varphi) \overset{df}{=} \begin{bmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{bmatrix}. \tag{9}$$

Если угол φ соизмерим с π, орбита $Orbit\, B(\varphi), \bar{b}^{(0)})$ конечна для любого начального значения $\bar{b}^{(0)} = (b_1^{(0)}, b_2^{(0)})$, а если φ несоизмерим с π, эта орбита бесконечна и всюду плотна на окружности $x^2 + y^2 = (b_1^{(0)})^2 + (b_2^{(0)})^2$, т.е. для любой точки $D(x_0, y_0)$, лежащей на этой окружности, для любого положительного числа ε в ε-окрестности точки D существует точка последовательности $\{(x^{(j)}, y^{(j)})\}_{j=0}^{\infty}$.

Доказательство очевидно.

Определение 6. Углы φ и ψ назовем π-эквивалентными, если $\varphi - \psi = r\pi$ для некоторого $r \in \mathrm{Rat}$.

Пусть B_0 и B_1 — операторы вида (9) поворота плоскости на углы φ_0, φ_1 и $Orbit\,(B_0, X_0)$, $Orbit\,(B_1, X_1)$ — их орбиты.

Лемма 2. Если углы φ_0 и φ_1 операторов поворота B_0, B_1 не являются π-эквивалентными и несоизмеримы с π, для любых точек $D_0(x_0, y_0)$, $D_1(x_1, y_1)$, лежащих на единичной окружности $x^2 + y^2 = 1$, для любого положительного числа ε в ε-окрестностях точек D_0, D_1 существуют точки орбит $Orbit\,(B_0, X_0)$, $Orbit\,(B_1, X_1)$ с одинаковыми номерами.

Доказательство. Пусть $\psi_0^{(0)}, \psi_1^{(0)}$ — начальные углы орбит операторов B_0, B_1; ψ^*_0, ψ^*_1 — углы точек D_0, D_1. Тогда действие операторов B_0, B_1 определяется формулами

$$\varphi_0^{(k)} = \psi_0 + k\varphi_0, \;\; \varphi_1^{(k)} = \psi_1 + k\varphi_1, \;\; k = 1, 2, \ldots$$

Рассмотрим разность $\varphi_1^{(k)} - \varphi_0^{(k)} = (\psi_1 - \psi_0) + k(\varphi_1 - \varphi_0), \;\; k = 1, 2, \ldots$

Обозначим $O(\varepsilon, \varphi)$ ε-окрестность угла φ, т.е. открытый интервал длины ε с центром в φ. Согласно лемме 1 для любого $\varepsilon > 0$ существует такое k_0, что $\varphi_1^{(k_0)} - \varphi_0^{(k_0)} \in O(\varepsilon/2, \psi_1^* - \psi_0^*)$. Далее, существует такое k_1, что $\varphi_0^{(k_0+k_1)} \in \in O(\varepsilon/2, \varphi_1^{(k_0)} - \varphi_0^{(k_0)})$. Это означает, что найдется такое наименьшее k_2, что $\psi_0^* \in O(\varepsilon/2, \varphi_0^{(k_0+k_2k_1)})$. Тогда $\varphi_0^{(k_0+k_2k_1)} \in O(\varepsilon, \psi_0^*)$, $\varphi_1^{(k_0+k_2k_1)} \in O(\varepsilon, \psi_1^*)$.

Лемма 3. Если углы $\varphi_1, \ldots, \varphi_k$ операторов поворота $B_1, \ldots, B_k$ не являются попарно π-эквивалентными и несоизмеримы с π, для любых точек $D_1(x_1, y_1), \ldots`, D_k(x_k, y_k)$, лежащих на единичной окружности $x^2 + y^2 = 1$, для любого положительного числа ε в ε-окрестностях $D_1, \ldots, D_k$ существуют точки орбит $Orbit\,(B_1, X_1), \ldots, Orbit(B_k, X_k)$ с одинаковыми номерами.

При доказательстве используется метод математической индукции и техника доказательства леммы 2.

Лемма 4. Пусть $(\bar{a}, X) = (\bar{a}_1, X_1) + \ldots + (\bar{a}_k, X_k)$ — линейная форма и $B_1, \ldots$ $\ldots, B_k$ — двумерные операторы поворота на углы $\varphi_1, \ldots, \varphi_k$ соответственно; причем эти углы не являются попарно π-эквивалентными и несоизмеримы с π. Определим действие оператора A следующим образом: $(\bar{a}, AX) = (\bar{a}_1, B_1X_1) + \ldots + (\bar{a}_k, B_kX_k)$,

а начальное значение $\bar{b} = (\bar{b}_1, \ldots, \bar{b}_k)$. Тогда

$$\operatorname*{Sup}_{X \in Orbit`(A,\, \bar{b})} (\bar{a}, X) = \operatorname*{Sup}_{X \in Orbit\,(B_1,\, \bar{b}_1)} (\bar{a}_1, X_1) + \ldots + \operatorname*{Sup}_{X \in Orbit\,(B_k, \bar{b}_k)} (\bar{a}_k, X_k)\,. \quad (10)$$

Доказательство. Для оператора (9) рассмотрим линейную форму $(\bar{a}, X) = a_1 x + a_2 y$. По условию, аргументы этой формы определены на окружности O радиуса $r = \sqrt{b_1^2 + b_2^2}$ с центром в начале координат. Форма $(\bar{a}, X)$ достигает своего максимума в точке $M(x_M, y_M)$ касания прямой $a_1 x + a_2 y = c$ к этой окружности, причем x_M, y_M и c вычисляются методами аналитической геометрии. Положим $d = \sqrt{a_1^2 + a_2^2}$. Нетрудно вычислить, что

$$x_M = \frac{a_1 r}{d},\ y_M = \frac{a_2 r}{d},\ \max = a_1 x_M + a_2 y_M = rd.$$

Согласно лемме 1 в любой ε-окрестности точки M существуют точки орбиты $Orbit\,(B, \bar{b})$. Поэтому

$$\operatorname*{Sup}_{X \in Orbit\,(B_1, \bar{b}_1)} (\bar{a}_1, X_1) = \max_{X \in O_1} (\bar{a}_1, X) = rd\,.$$

Пусть $M_1, \ldots, M_k$ — точки максимума для форм $(\bar{a}_1, X_1), \ldots, (\bar{a}_k, X_k)$ на O_1. По лемме 3 для системы этих точек и любого положительного ε в ε-окрестностях этих точек существуют точки $D_1, \ldots, D_k$ орбит операторов $B_1, \ldots, B_k$ с начальными значениями $\bar{b}_1, \ldots, \bar{b}_k$ соответственно. Поэтому для вычисления $\operatorname*{Sup}_{X \in Orbit\,(A,\, \bar{b})} (\bar{a}, X)$ следует вычислить $\max_{X \in O_1} (\bar{a}_i, X_i)$ и использовать равенство (10).

Лемма 5. Пусть линейная форма $(\bar{a}, X)$, двумерные операторы $B_1, \ldots, B_k$, оператор A и начальное значение $\bar{b}$ определены так же, как в лемме 4. Тогда задачу вычисления $\operatorname*{Sup}_{X \in Orbit\,(A,\, \bar{b})} (\bar{a}, X)$ можно свести к вычислениям по формуле (10).

Доказательство. Предположим, что $\varphi_1, \ldots, \varphi_l$ — класс эквивалентности φ_1 по отношению π-эквивалентности $\varphi_i \sim \varphi_j \leftrightarrow \varphi_i - \varphi_j = r_{ij}\pi$, $r_{ij} \in \mathrm{Rat}$. Поскольку точки орбит всех операторов B_i лежат на единичной окружности, можно считать, что $\begin{bmatrix} x_i \\ y_i \end{bmatrix} = R_i \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$, где R_i — операторы поворота на углы $r_{1i}\pi$. Поэтому $(\bar{a}_1, X_1) + \ldots + (\bar{a}_l, X_l) = (\bar{a}_1 + \bar{a}_2 R_2 + \ldots + \bar{a}_l R_l) X_1$, а $(\bar{a}_1, B_1 X_1) + \ldots + (\bar{a}_l, B_l X_l) = (\bar{a}_1 B_1 + \bar{a}_2 R_2 B_2 + \ldots + \bar{a}_l R_l B_l) X_1$. Таким образом, все слагаемые линейной формы с π-эквивалентными углами можно выразить через одну линейную форму и в формуле (10) можно считать все углы попарно неэквивалентными.

Лемма 6. Пусть $f(x) \in K[x]$ — многочлен и $\lambda_1, \ldots, \lambda_k$ — комплексные корни $f(x)$ такие, что $|\lambda_1| = \ldots = |\lambda_k| = 1$, $\lambda_j = \cos(\varphi_j) + i \sin(\varphi_j)$, $j = 1, \ldots, k$. Тогда проблема вычисления классов π-эквивалентности на множестве $\varphi_1, \ldots, \varphi_k$ алгоритмически разрешима.

Доказательство. Пусть $\varphi,\ \psi \in \{\varphi_1, \ldots, \varphi_k\}$, $\varphi - \psi = r\pi$, $r \in \mathrm{Rat}$, $\lambda = \cos(\varphi) + i \sin(\varphi)$, $\mu = \cos(\psi) + i \sin(\psi)$, $\lambda / \mu = \cos(\varphi - \psi) + i \sin(\varphi - \psi) = \cos(r\pi) + i \sin(r\pi)$ — корень некоторой степени из единицы. Алгоритмы арифметических действий над алгебраическими числами изложены, например, в [23]. Основная идея состоит в следующем: определим систему полиномиальных равенств $(f(u) = 0) \,\&\, (f(v) = 0) \,\&\, (wv - u = 0)$ и исключим из нее переменные u, v методами теории исключений [22] или базисов Гребнера [23]. В результате имеем многочлен $h(w)$, один из делителей

которого должен быть минимальным многочленом некоторого корня из единицы. Таким образом, $\deg(\mathrm{Gcd}(w^d - 1, h(w))) > 0$ для некоторого натурального $d \le \deg(h)$.

Лемма 7. Пусть $f(x) \in K[x]$ — многочлен и $\lambda_1, \ldots, \lambda_n$ — его корни. Тогда проблема распознавания количества k корней таких, что $|\lambda_1| = \ldots = |\lambda_k|$ и $|\lambda_1| = \max(|\lambda_1| = \ldots = |\lambda_n|)$, алгоритмически разрешима.

Доказательство. Положим $x = u + iv$. Тогда $f(x)$ можно переписать, выделив действительную и мнимую части $f(x)$: $f(u+iv) = \mathrm{re}\, f(u, v) + i \cdot \mathrm{im}\, f(u, v)$. Поскольку $|x|^2 = u^2 + v^2$, задачу определения чисел с равными модулями можно сформулировать в виде системы равенств

$$(\mathrm{re}\, f(u, v) = 0) \& (\mathrm{im}\, f(u, v) = 0) \& (w - u^2 - v^2 = 0). \qquad (11)$$

Так как переменная v входит в $\mathrm{im}\, f(u, v)$ в нечетной степени, то $\mathrm{im} f(u, v) = v \cdot \mathrm{im} f_1(u, v)$.

Положив $v = 0$, получим $\mathrm{re}\, f(u,0) = f(u)$. Таким образом, (11) упростится до системы $(f(u) = 0) \& (w - u^2 = 0)$. Иными словами, для этого случая задача сводится к отделению и вычислению кратностей действительных корней $f(x)$.

При $v \ne 0$ система (11) упростится до $(\mathrm{re}\, f(u, v) = 0) \& (\mathrm{im}\, f_1(u, v) = 0) \&$ $\& (w - u^2 - v^2 = 0)$. Поскольку переменная v входит в эту систему в четной степени, при исключении переменных алгоритм оперирует по сути с переменной $v_1 = v^2$. Исключив из системы переменные u, v^2, получим полиномиальное равенство $g(w) = 0$, действительные корни которого — суть квадраты модулей комплексной части чисел $\lambda_1, \ldots, \lambda_n$. Теперь задача сводится к отделению и определению кратностей корней $g(w) = 0$. Если λ_i — максимальный действительный корень $f(x)$, а λ_j — максимальный действительный корень $g(x)$ и $\lambda_i = \lambda_j$, то $\deg(\mathrm{Gcd}(f, g)) > 0$ и λ_i — действительный корень $\mathrm{Gcd}(f, g)$. Пусть p — кратность λ_i, а q — кратность λ_j и $\lambda_i = \lambda_j$. Тогда кратность λ_i равна $p + 2q$. Если $\lambda_i \ne \lambda_j$, кратность искомого максимального корня равна либо p (случай 1), либо $2q$ (случай 2).

Пример 2. Рассмотрим алгоритмы алгебраических вычислений задачи доказательства инвариантности неравенства, считая, что

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{bmatrix}.$$

1. Вычисление характеристического многочлена:

$$f(x) = |A - xE| = \begin{bmatrix} -x & 1 & 0 \\ 0 & -x & 1 \\ 2 & 0 & -x \end{bmatrix} = -x^3 + 2, \quad f(x) = x^3 - 2,$$

$$\lambda_1 = \sqrt[3]{2}, \quad \lambda_2 = \sqrt[3]{2} * \varepsilon, \quad \lambda_3 = \sqrt[3]{2} * \varepsilon^2,$$

$\varepsilon = \cos\left(\frac{2\pi}{3}\right) + i * \sin\left(\frac{2\pi}{3}\right)$, ε — первообразный корень степени 3 из единицы.

2. Алгоритм леммы 7. Система уравнений леммы 7:

$$f(u + iv) = \mathrm{re}\, f(u, v) + i \cdot \mathrm{im}\, f(u, v);$$

$$(\mathrm{re}\, f(u, v) = 0) \& (\mathrm{im}\, f(u, v) = 0) \& (w - u^2 - v^2 = 0);$$

$$x^3-2=0 \rightarrow (u+iv)^3-2=0;$$

$$\begin{cases}(u^3-3uv^2-2)=0\\ 3u^2v-v^3=0\end{cases}\rightarrow\begin{cases}u^3-3uv^2-2=0\\ 3u^2-v^2=0\end{cases}\text{(случай 1)}\vee\begin{cases}u^3-2=0\\ v=0\end{cases}\text{(случай 2).}$$

Случай 1:

$$\begin{cases}u^3-3uv^2-2=0\\ 3u^2-v^2=0\\ w=u^2+v^2\end{cases}\rightarrow\begin{cases}v^2=\dfrac{u^3-2}{3u}\\ 3u^2-v^2=0\\ w=u^2+v^2\end{cases}\rightarrow\begin{cases}uv^2+\dfrac{3}{4}=0\\ 4u^3+1=0\\ w^3-4=0\end{cases}.$$

Итак, $q=1$, $p=1$. Многочлен $f(x)=x^3-2$ имеет $p+2q=3$ корня с максимальным модулем.

3. Алгоритм леммы 6.

3.1. Проверка соизмеримости угла φ с π. Имеем систему $(f(x)=0)\&$ $\&\,(f(w^2)=0)\&\,(x-uw=0)$,

$$\begin{cases}x^3-2=0\\ w^6-4=0\\ x-uw=0\end{cases}\rightarrow\begin{cases}x^3-2=0\\ w^3-2=0\\ x-uw=0\end{cases}\rightarrow\begin{cases}(uw)^3-2=0\\ w^3-2=0\\ x-uw=0\end{cases}\rightarrow\begin{cases}u^3-1=0\\ w^3-2=0\\ x-uw=0\end{cases}\rightarrow$$

$$\rightarrow \operatorname{Gcd}(u^3-1,u^2+u+1)=u^2+u+1\rightarrow\varphi=2\pi/3,$$

т.е. φ соизмерим с π.

3.2. Проверка соизмеримости разности углов $\varphi_u-\varphi_v$ с π. Система имеет вид $(f(u)=0)\&\,(f(v)=0)\&\,(wv-u=0)$,

$$\begin{cases}u^3-2=0\\ v^3-2=0\\ wv-u=0\end{cases}\rightarrow\begin{cases}w^3v^3-2=0\\ v^3-2=0\\ wv-u=0\end{cases}\rightarrow\begin{cases}w^3-1=0\\ v^3-2=0\\ wv-u=0\end{cases}\rightarrow$$

$$\rightarrow \operatorname{Gcd}(w^3-1,w^2+w+1)=w^2+w+1\rightarrow\varphi_u-\varphi_v=2\pi/3,$$

т.е. углы φ_u, $\varphi_v-\pi$ π-эквивалентны.

3.3. Представление AX для линейной формы вида (7):

$$A\begin{bmatrix}x\\ y\\ z\end{bmatrix}=\left(\sqrt[3]{2}\begin{bmatrix}\cos(2\pi/3) & \sin(2\pi/3)\\ -\sin(2\pi/3) & \cos(2\pi/3)\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix},\sqrt[3]{2}z\right)^{\mathrm{T}}.$$

3.4. Вычисление матрицы перехода к жордановой форме.

— Вычисление собственных векторов матрицы $A=\begin{pmatrix}0&1&0\\ 0&0&1\\ 2&0&0\end{pmatrix}$.

Решить систему однородных линейных уравнений $(A-\lambda E)(x,y,z)^{\mathrm{T}}=0$, причем вычисления осуществляются в поле $K(\lambda)$ по модулю λ^3-2.

Ранг системы $\begin{cases}\lambda x-2z=0\\ x-\lambda y=0\\ y-\lambda z=0\end{cases}$ равен двум. Фундаментальное решение системы

есть вектор $s=(\lambda^2,\lambda,1)$. Собственные векторы оператора A:

$$s_1=(\lambda_1^2,\lambda_1,1),\ s_2=(\lambda_2^2,\lambda_2,1),\ s_3=(\lambda_3^2,\lambda_3,1).$$

— Вычисление матрицы перехода S и обратной матрицы S^{-1}:

$$S=\begin{bmatrix}\lambda_1^2 & \lambda_2^2 & \lambda_3^2\\ \lambda_1 & \lambda_2 & \lambda_3\\ 1 & 1 & 1\end{bmatrix},\ S^{-1}=\frac{1}{\det(S)}\begin{bmatrix}\lambda_2-\lambda_3 & \lambda_2^2-\lambda_3^2 & \lambda_2^2\lambda_3-\lambda_2\lambda_3^2\\ \lambda_1-\lambda_3 & \lambda_1^2-\lambda_3^2 & \lambda_1^2\lambda_3-\lambda_1\lambda_3^2\\ \lambda_1-\lambda_2 & \lambda_1^2-\lambda_2^2 & \lambda_1^2\lambda_2-\lambda_1\lambda_2^2\end{bmatrix}.$$

Теорема 1. Проблема доказательства инвариантности неравенства (4) для цикла (1) с диагонализируемым линейным оператором A и с данной начальной точкой $\bar{b}$ алгоритмически разрешима.

Доказательство. Поскольку оператор A диагонализируем, представление $(\bar{a},A^mX)$ имеет вид

$$(\bar{a},A^mX)=r_1^m(\bar{a}_1,\hat{B}_1^mX_1)+\ldots+r_k^m(\bar{a}_k,\hat{B}_k^mX_k)+\lambda_{2k+1}^m a_{2k+1}x_{2k+1}+\ldots+\lambda_n^m a_n x_n\ . \quad (12)$$

Пусть p и q — числа, определенные в лемме 7 для характеристического полинома $f(x)$ оператора A. Для определенности будем считать, что собственные числа оператора A с максимальными модулями имеют начальные номера $\lambda_1,\lambda_2,\ldots,\lambda_{2q-1},\lambda_{2q},\lambda_{2q+1},\ldots,\lambda_{2q+p}$, причем $\lambda_1=\bar{\lambda}_2,\ldots,\lambda_{2q-1}=\bar{\lambda}_{2q}$. Тогда (12) можно представить в виде

$$(\bar{a},A^mX)=$$

$$=r_1^m(\bar{a}_1,\hat{B}_1^mX_1)+\ldots+r_q^m(\bar{a}_q,\hat{B}_q^mX_q)+\lambda_{2q+1}^m a_{2q+1}x_{2q+1}+\ldots+\lambda_{2q+p}^m a_{2q+p}x_{2q+p}+L_1^{(m)},$$

где $L_1^{(m)}$— m-я итерация линейной формы вида (12) от оставшихся переменных. Неравенство (4) можно переписать в виде

$$(\bar{a}_1,\hat{B}_1^mX_1)+\ldots+(\bar{a}_q,\hat{B}_q^mX_q)+$$

$$+\varepsilon_{2q+1}^m a_{2q+1}x_{2q+1}+\ldots+\varepsilon_{2q+p}^m a_{2q+p}x_{2q+p}+\frac{1}{r_1^m}L_1^{(m)}\le\frac{1}{r_1^m}(\bar{c},\bar{b}).$$

Обозначим $L_0^{(m)}$ линейную форму

$$(\bar{a}_1,\hat{B}_1^mX_1)+\ldots+(\bar{a}_q,\hat{B}_q^mX_q)+\varepsilon_{2q+1}^m a_{2q+1}x_{2q+1}+\ldots+\varepsilon_{2q+p}^m a_{2q+p}x_{2q+p},$$

где $\varepsilon_j=\pm1$. Получим

$$L_0^{(m)}+\frac{1}{r_1^m}L_1^{(m)}\le\frac{1}{r_1^m}(\bar{c},\bar{b}). \quad (13)$$

Так как $r_1>\max(|\lambda_{2p+q+1}|,\ldots,|\lambda_n|)$, при $m\to\infty$ имеем $\frac{1}{r_1^m}L_1\to0$. Следовательно, для любого $\delta>0$ существует такое натуральное число m_0, что при $m>m_0$ имеем $\left|\frac{1}{r_1^m}L_1^{(m)}\right|<\delta$.

Имеют место следующие случаи.

1. Если $r_1 < 1$, то $\lim\limits_{m\to\infty} \dfrac{1}{r_1^m}(\bar{c}, \bar{b}) = \infty$. Тогда:

— при $(\bar{c}, \bar{b}) < 0$ для любого $\varepsilon > 0$ существует такое $m_1 < m$, при котором

$$L_0^{(m)} + \frac{1}{r_1^m} L_1^{(m)} < L_0^{(m)} + \delta < -\varepsilon,$$

т.е. при $m > \max(m_0, m_1)$ неравенство (4) не выполняется;

— при $(\bar{c}, \bar{b}) > 0$ имеем $L_0^{(m)} + \dfrac{1}{r_1^m} L_1^{(m)} < L_0^{(m)} + \delta < +\infty$, т.е. при $m > \max(m_0, m_1)$ неравенство (4) выполняется.

2. Если $r_1 = 1$, то $\lim\limits_{m\to\infty} \dfrac{1}{r_1^m}(\bar{c}, \bar{b}) = (\bar{c}, \bar{b})$. При $m > m_0$ имеем $L_0^{(m)} + \dfrac{1}{r_1^m} L_1^{(m)} < L_0^{(m)} + \delta < (\bar{c}, \bar{b})$. Следовательно, при $m > m_0$ для выполнения неравенства (4) должно выполняться условие $L_0^{(m)} < (\bar{c}, \bar{b})$.

3. Если $r_1 > 1$, то $\lim\limits_{m\to\infty} \dfrac{1}{r_1^m}(\bar{c}, \bar{b}) = 0$. При $m > m_0$ имеем $L_0^{(m)} + \dfrac{1}{r_1^m} L_1^{(m)} < L_0^{(m)} + \delta < 0$. Следовательно, для выполнения неравенства (4) при $m > \max(m_0, m_1)$ должно выполняться условие $L_0^{(m)} < 0$.

Неравенство вида $L_0^{(m)} < c$ для произвольного c на произвольном множестве S эквивалентно $\operatorname{Sup}\limits_{X\in S} L_0^{(m)} < c$. Поэтому независимо от случаев 1–3, доказательство инвариантности сводится к вычислению

$$\operatorname{Sup}_{X\in Orbit(A,\bar{b})} L_0^{(m)},$$

$$L_0^{(m)} = (\bar{a}_1, \hat{B}_1^m \bar{b}_1) + \ldots + (\bar{a}_q, \hat{B}_q^m \bar{b}_q) + \varepsilon_{2q+1}^m a_{2q+1} b_{2q+1} + \ldots + \varepsilon_{2q+p}^m a_{2q+p} b_{2q+p}.$$

Алгоритм вычисления $\operatorname{Sup}\limits_{X\in Orbit(A,\bar{b})} (\bar{a}_1, \hat{B}_1^m \bar{b}_1) + \ldots + (\bar{a}_q, \hat{B}_q^m \bar{b}_q)$ приведен в леммах 4, 6. Вычисление линейной части $\operatorname{Sup}\limits_{X\in Orbit(A,\bar{b})} \varepsilon_{2q+1}^m a_{2q+1} b_{2q+1} + \ldots + \varepsilon_{2q+p}^m a_{2q+p} b_{2q+p}$ осуществляется непосредственно для четного и нечетного значений m.

Общий алгоритм доказательства инвариантности неравенства (4) для цикла (1) и данного начального значения $\bar{b}$ заключается в следующем.

Шаг 1. Привести неравенство к виду (13).

Шаг 2. Вычислить значение $m^* = \max(m_0, m_1)$ и определить принадлежность к одному из вариантов: 1, 2 или 3.

Шаг 3. Проверить выполнение условия инвариантности для случая, определенного в п. 2, и для значений $m > m^*$.

Шаг 4. Проверить неравенство (4), выполняя цикл (1) для всех значений $m \le m^*$.

Пример 3 (продолжение примера 1).

Напомним, что

$$S(b_1, b_2) = (0 \le b_1 \le 1) \& (0 \le b_2 \le 1), \quad U(x, y, b_1, b_2) = \neg(|x + b_1| \le \varepsilon) \& (|y + b_2| \le \varepsilon),$$

$$A = \begin{bmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{bmatrix}, \quad L = x + y \le 2b_1 + 2b_2 \,//\, \bar{a} = (1, 1), \quad \bar{c} = (2, 2).$$

Выполним шаг 1.

— Вычислить характеристический многочлен

$$A = \begin{bmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{bmatrix}, \quad |A - xE| = \begin{vmatrix} 3/5 - x & 4/5 \\ -4/5 & 3/5 - x \end{vmatrix} = x^2 - 6/5x + 1.$$

— Найти количество корней с максимальным модулем:

$$x^2 - 6/5x + 1 = 0 \;\rightarrow\; (u + iv)^2 - 6/5(u + iv) + 1 = 0,$$

$$\begin{cases} u^2 - v^2 + 6/5u + 1 = 0 \\ 2uv - 6/5v = 0 \end{cases} \rightarrow \begin{cases} u^2 - v^2 + 6/5u + 1 = 0 \\ u - 3/5 = 0 \end{cases} \text{(случай 1)} \vee \begin{cases} u^2 + 6/5u + 1 = 0 \\ v = 0 \end{cases} \text{(случай 2)}.$$

Вычислим случай 1 (случай 2 тривиален):

$$\begin{cases} u^2 - v^2 + 6/5u + 1 = 0 \\ u - 3/5 = 0 \\ w = u^2 + v^2 \end{cases} \rightarrow \begin{cases} 9/25 - v^2 + 18/25 + 1 = 0 \\ u - 3/5 = 0 \\ w = u^2 + v^2 \end{cases} \rightarrow \begin{cases} v^2 - 16/25 = 0 \\ u - 3/5 = 0 \\ w = 1 \end{cases}.$$

Итак, $q = 1$, $p = 0$. Многочлен $f(x) = x^2 - 6/5x + 1$ имеет $p + 2q = 2$ комплексных корня с максимальным модулем, равным единице.

— Проверить соизмеримость угла φ с π: $(f(x) = 0) \& (f(w^2) = 0) \& (x - uw = 0)$,

$$\begin{cases} x^2 - 6/5x + 1 = 0 \\ w^2 - 1 = 0 \\ x - uw = 0 \end{cases} \rightarrow \begin{cases} x^2 - 6/5x + 1 = 0 \\ w - 1 = 0 \\ x - u = 0 \end{cases} \rightarrow \begin{cases} u^2 - 6/5u + 1 = 0 \\ w - 1 = 0 \\ x - u = 0 \end{cases} \rightarrow$$

$$\rightarrow \text{Gcd}\,(u^2 - 6/5u + 1 = 0, u - 1) = 1,$$

т.е. φ несоизмерим с π.

— Проверить соизмеримость разности углов $\varphi_u - \varphi_v$ с π: $(f(u) = 0) \& (f(v) = 0) \& (wv - u = 0)$,

$$\begin{cases} u^2 - 6/5u + 1 = 0 \\ v^2 - 6/5v + 1 = 0 \\ wv - u = 0 \end{cases} \rightarrow \begin{cases} v = (w + 1)/(6/5w) \\ v^2 - 6/5v + 1 = 0 \\ wv - u = 0 \end{cases} \rightarrow \begin{cases} v = (w + 1)/(6/5w) \\ 25w^2 + 14w + 25 = 0 \\ wv - u = 0 \end{cases} \rightarrow$$

$$\rightarrow \text{Gcd}\,(25w^2 + 14w + 25,\; w^2 - 1) = 1,$$

т.е. φ_u и φ_v не являются π-эквивалентными.

— Представить A в вещественной жордановой форме. Поскольку A уже представлена в требуемой форме, то $S = E$.

Выполним шаг 2.

— Вычислить по лемме 4 равенство $\sup\limits_{(x,y)\in Orbit\,(A,\,\bar{b})} (\bar{a},\,(x,\,y)^{\mathrm{T}}) = \sqrt{2}\sqrt{b_1^2+b_2^2}$.

— Поскольку $|\lambda| = w = 1$, имеет место случай 2 доказательства теоремы 1.

Выполним шаг 3.

— Согласно теореме 3 неравенство (4) должно выполняться для всех вершин предусловия $S(\bar{b})$, т.е. по лемме 4

$$\sup_{(x,y)\in O(b_1,b_2)} (x+y) \le b_1+b_2 \ \text{ для } \ (b_1,b_2)=(0,0),\ (b_1,b_2)=(0,1),$$
$$(b_1,b_2)=(1,0),\ (b_1,b_2)=(1,1).$$

Проверка: $\sqrt{2}\cdot 0 \le 0,\ \sqrt{2}\sqrt{b_1^2+b_2^2} = \sqrt{2} \le 2,\ \sqrt{2}\sqrt{b_1^2+b_2^2} = \sqrt{2} \le 2, \sqrt{2}\sqrt{b_1^2+b_2^2} = 2 \le 4$.

Таким образом, неравенство $(\bar{a},\,X) \le (\bar{c},\,\bar{b})$ выполняется для всех $\bar{b} \in S(\bar{b})$.

Поскольку вещественная жорданова форма состоит из одной 2×2 клетки, перехода к пределу в теореме 1 и вычисления m^* не требуется.

МЕТОД ПРОВЕРКИ ИНВАРИАНТНОСТИ НЕРАВЕНСТВА В ОБЩЕМ СЛУЧАЕ

Теорема 2. Проблема доказательства инвариантности неравенства (4) для цикла (1) с данной начальной точкой $\bar{b}$ алгоритмически разрешима.

Доказательство заключается в расширении рассуждений теоремы 1 на случай матрицы A с нетривиальными жордановыми клетками. Пусть матрица оператора A в жордановой форме имеет нетривиальные жордановы клетки. Поскольку для каждого комплексного собственного значения λ существует сопряженное собственное значение $\bar{\lambda}$, жорданова форма A наряду с клеткой $J_k(\lambda)$ содержит клетку $J_k(\bar{\lambda})$. Подматрица вещественной жордановой формы оператора A, соответствующая паре $(\lambda,\bar{\lambda})$, имеет вид

$$J(\lambda)=\begin{bmatrix} B(\varphi) & E & \dots & 0 \\ 0 & B(\varphi) & \dots & 0 \\ . & . & . & . \\ 0 & \dots & B(\varphi) & E \\ 0 & \dots & 0 & B(\varphi) \end{bmatrix},\ B(\varphi)=r\begin{bmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{bmatrix},\ E=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

и матрица оператора A имеет вид $A = J_1(\lambda_1)\times\ldots\times J_l(\lambda_l)\times J_{l+1}(\lambda_{l+1})\times\ldots$ $\ldots\times J_{l+k}(\lambda_{l+k})$, где $\lambda_1,\bar{\lambda}_1\ldots\lambda_l,\bar{\lambda}_l$ являются комплексными собственными числами, а $\lambda_{l+1},\ldots,\lambda_{l+k}$ — вещественные собственные числа A:

$$A^m = J_1^m(\lambda_1)\times\ldots\times J_l^m(\lambda_l)\times J_{l+1}^m(\lambda_{l+1})\times\ldots\times J_{l+k}^m(\lambda_{l+k}). \qquad (14)$$

Каждой клетке $J_j(\lambda_j)$ соответствует своя группа переменных. Поэтому рассмотрим жорданову клетку размера k, обозначенную в (14). Элементы этой клетки — 2×2 матрицы. Пусть $X=(X_1,\ldots,X_k), X_j=(x_{2j-1},x_{2j})$. Пара (x_{2j-1},x_{2j}) соответствует паре сопряженных собственных чисел $(\lambda_j,\bar{\lambda}_j)$. Пусть m — натуральное число и $\bar{b}=(\bar{b}_1,\ldots,\bar{b}_k)$, $\bar{b}_j=(b_{2j-1},b_{2j})$ — вектор пар переменных — начальных значений. Вычислим m-ю итерацию $X^{(0)}=\bar{b}$; $X^{(m)}=AX^{(m)}$ в явном виде; $X^{(m)}=A^mX$: $X^{(m)}=J(\lambda)^m\bar{b}$. Получим

$$X^{(m)} = \begin{bmatrix} r^m B(m\varphi) & C_1(m) & \dots & C_{k-1}(m) \\ 0 & r^m B(m\varphi) & \dots & C_{k-2}(m) \\ 0 & \dots & r^m B(m\varphi) & C_1(m) \\ 0 & \dots & 0 & r^m B(m\varphi) \end{bmatrix} \begin{bmatrix} \bar{b}_1 \\ \bar{b}_2 \\ \dots \\ \bar{b}_k \end{bmatrix}, \; b_j = \begin{bmatrix} b_{2j-1} \\ b_{2j} \end{bmatrix}, \quad (15)$$

где $C_j(m) = C_m^j r^{m-j} B((m-j)\varphi) = \dfrac{m(m-1)\dots(m-j+1)}{j!} r^{m-j} B((m-j)\varphi)$, $j \in 1, \dots, k-1$.

Равенство, соответствующее j-й строке (15), имеет вид

$$x_j^{(m)} = r^m \left(\bar{b}_j B(m\varphi) + \frac{C_1(m)}{r} \bar{b}_{j+1} + \dots + \frac{C_{k-j}(m)}{r^{k-j}} \bar{b}_k \right) \overset{df}{=} r^m g_j(m, r, b). \quad (16)$$

Линейная форма — аналог (6) представляет собой сумму, каждое слагаемое которой определено группой переменных клетки $J_j(\lambda_i)$:

$$r_j^m S_j^{(m)} = r_j^m (g_1(m, r_j, b_{j1}) a_{j1} + g_2(m, r_j, b_{j2}) a_{j2} + \dots + g_{k_j}(m, r_j, b_{jk_j}) a_{jk_j}). \quad (17)$$

Аналог линейного неравенства (4) имеет вид

$$r_1^m S_1^{(m)} + r_2^m S_2^{(m)} + \dots + r_l^m S_l^{(m)} \le c. \quad (18)$$

Обозначим r_1 максимальное значение: $r_1 = \max(|\lambda_1|, \dots, |\lambda_l|)$. Тогда поскольку $S_j^{(m)}$ — многочлен от m, а $(r_j / r_1)^m$ — показательная функция от m и $r_j / r_1 < 1$, имеем

$$\frac{r_j^m S_j^{(m)}}{r_1^m} \underset{m \to \infty}{\to} 0 \text{ при } r_j \ne r_1, \; \frac{r_1^m S_1^{(m)}}{r_1^m} \underset{m \to \infty}{\to} \bar{b} B_1(m\varphi).$$

Поэтому метод из теоремы 1 может быть использован и в данной теореме, т.е. в общем случае.

Теорема 3. Проблема доказательства инвариантности неравенства (4) для цикла (1) (т.е. с данным предусловием $S(b)$) алгоритмически разрешима.

Доказательство. Линейное полуалгебраическое множество $S = \{\bar{b} \mid S(\bar{b})\}$ можно представить в виде объединения выпуклых многогранных множеств, поскольку $S(b)$ можно представить в виде $S_1(b) \vee \dots \vee S_l(b)$ — систем линейных неравенств. В [19, леммы 2, 3] доказано, что выполнение линейного неравенства для любой точки выпуклого многогранника следует из его выполнения на всех вершинах этого многогранника. Поэтому доказательство инвариантности $L(\bar{a}, \bar{c}, A^m X, \bar{b})$ на $S(b)$ заключается в его проверке для всех $S_1(b), \dots, S_l(b)$.

Теорема 4. Проблема завершаемости цикла (1) алгоритмически разрешима.

Доказательство. Цикл (1) расходится тогда и только тогда, когда условие $U(x, b)$ — инвариант цикла (2).

ЗАКЛЮЧЕНИЕ

Настоящая работа — прямое продолжение [19]. Рассмотрение линейного оператора с комплексными собственными числами приведено в леммах 1–7 теоремы 1. В данной статье, как и в [19], изложена только основная идея метода. Алгоритмы компьютерной линейной алгебры, оценки числа m итераций метода, алгоритмы отделения и уточнения корней многочленов, проверки инвариантности первых m соотношений в точках орбиты (3) здесь не обсуждаются. Изложение методов компьютерной алгебры содержится, например, в [21–23].

Можно предположить, что метод может быть положен в основу 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 Applied Mathematics / J.T. Schwartz (Ed.). — Providence, R.I.: American Mathematical Society, 1967. — **19**. — P. 19–32.
2. Hoare C.A.R. An axiomatic basis for computer programming // Communications of the ACM. — 1969. — **12**, N 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 // Applicable Algebra in Engineering, Communication and Computing. — 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. Technical Report N 07-07 in RISC Report Series, University of Linz, Austria. 06 2007. Workshop Proceedings. — P. 85–99.
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 // Proceedings of the 31st ACM SIGPLAN-SIGACT Symposium on Principles of Programming 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 Symposium on Principles of Programming Languages. — Venice, Italy, January 14–16, 2004. — New York: ACM, 2004. — P. 318–329.
10. Rodríguez-Carbonell E., Kapur D. Automatic generation of polynomial loop invariants: algebraic foundations // Proc. of International Symposium on Symbolic and Algebraic Computation. — 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 Scientific Computing. — Timisoara, Romania, Sept. 25–29, 2005. IEEE Computer Society, 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 // Conference Record of the Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, Tucson, Arizona. — New York: ACM Press, 1978. — 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.Б., Капитонова Ю.В., Кривой С.Л., Летичевский А.А. Итеративные методы анализа программ. Равенства и неравенства // Кибернетика. — 1990. — № 3. — С. 1–10.
17. Львов М.С. Инвариантные неравенства в программах, интерпретированных над упорядоченными полями // Кибернетика. — 1986. — № 5. — С. 22–27.
18. Львов М.С. Об инвариантных неравенствах для состояний схем программ, интерпретированных над векторным пространством // Кибернетика. — 1985. — № 2. — С. 111–112.
19. Львов М.С. Метод доказательства инвариантности линейных неравенств для линейных циклов // Кибернетика и системный анализ. — 2014. — **50**, № 4. — С. 80–85 .
20. Робинсон А. Введение в теорию моделей и метаматематику алгебры. — М.: Наука, ГРФМЛ, 1967. — 376 с.
21. Ван дер Варден Б.Л. Алгебра. — 2-е изд. — М.: Мир, 1976. — 648 с.
22. Ходж В., Пидо Д. Методы алгебраической геометрии. Т. 1. — М.: ИЛ, 1954. — 462 с.
23. Компьютерная алгебра: символьные и алгебраические вычисления / Под ред. Б. Бухбергера, Дж. Коллинза, Р. Лооса. — М.: Мир, 1986. — 392 с.

Поступила 29.12.2014