УДК 004.421.6

М.С. ЛЬВОВ

ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ ЛИНЕЙНЫХ ЦИКЛОВ

Ключевые слова: *статический анализ программ, полиномиальные инварианты циклов, задача автоматической генерации.*

ВВЕДЕНИЕ

Проблема поиска инвариантов циклов в императивных программах поставлена в работах Р. Флойда [1] и С. Хоара [2] как ключевая проблема процесса анализа свойств программ. Отметим, что существование и эффективность алгоритмов генерации программных инвариантов зависят от предметной области, т.е. от свойств алгебр данных, с которыми работает программа. Исследования задачи автоматической генерации программных инвариантов для различных алгебр данных выполнялись начиная с 70-х годов в Институте кибернетики; их основные результаты представлены в [3, 4].

Наиболее важные с точки зрения практики — числовые алгебры данных. В работе [5] изложены два метода построения полиномиальных инвариантов типа равенств в программах, алгеброй данных которых является область целостности (полиномиально определенные программы) или поле (рационально определенные программы). Один из них заключается в построении алгебраических зависимостей между функциями — правыми частями оператора присваивания в теле цикла; другой — метод неопределенных коэффициентов — строит все инварианты данного вида в произвольной контрольной точке программы. Вид инварианта задается полиномиальной формой с неопределенными коэффициентами. Метод основан на свойстве нетеровости колец полиномов многих переменных.

Эту идею M. Müller-Olm и H. Seidl использовали в [6] при решении задачи построения полиномиальных инвариантов ограниченной степени для полиномиально определенных программ. При этом учитываются программные условия типа $f(X) \neq 0$, где $f(X)$ — многочлены от переменных программы. Те же авторы [7] предложили метод вычисления полиномиальных программных инвариантов ограниченной степени в линейно-определенных (аффинных) программах, содержащих рекурсивные вызовы процедур.

В работе [8] S. Sankaranarayanan, H. Sipma, Z. Manna представили метод вычисления полиномиальных инвариантов циклов в виде полиномиальных форм (template polynomlals) с использованием алгоритма вычисления базисов Гребнера. M. Caplain [9] описал метод построения нелинейных и, вообще говоря, неполиномиальных инвариантных соотношений для линейных циклов. Метод использует собственные значения и собственные векторы линейного оператора в теле цикла.

Алгебраические основы задачи поиска полиномиальных инвариантов циклов изложили в [10] E. Rodriguez-Carbonell и D. Kapur. Основной результат этой работы — алгоритм вычисления всех полиномиальных инвариантов для циклов с так называемыми разрешимыми операторами присваивания. В частности, разрешимыми являются аффинные операторы с положительными вещественными собственными значениями. Эти же авторы в [11] предложили метод генерации полиномиальных инвариантов циклов, включая вложенные циклы, а также программные условия как в виде полиномиальных равенств, так и неравенств. В статье рассматривается большое количество примеров; приводятся таблицы времени работы алгоритма в зависимости от технических параметров анализируемых программ.

В работе [12] L. Kovács, T. Jebelean предложили алгоритм поиска инвариантов циклов, основанный на построении системы рекуррентных соотношений от переменных цикла и параметра n — числа повторений цикла. Алгоритм ищет решение этой системы, зависящее от n. Он реализован в программной системе Теорема (Theorema System); его работа подробно иллюстрирована примерами.

L-ИНВАРИАНТЫ ЛИНЕЙНЫХ ОТОБРАЖЕНИЙ И ИНВАРИАНТЫ ЛИНЕЙНЫХ ЦИКЛОВ

Определение 1. Пусть W — n-мерное векторное пространство над полем рациональных чисел Q и $\overline{Q}$ — алгебраическое замыкание поля Q. Обозначим $X=(x_1,\dots,x_n)$ n-мерный вектор переменных. Рациональная функция $p(X)\in\overline{Q}(X)$ называется L-инвариантом линейного оператора $A: W\to W$, если для любого вектора $b\in W$ имеет место соотношение

$$p(Ab)=p(b). \tag{1}$$

Пример 1 (линейный оператор с характеристическим многочленом x^3-2). Рассмотрим линейный оператор с матрицей

$$A=\begin{pmatrix}0&1&0\\0&0&1\\2&0&0\end{pmatrix},\quad X=(x,y,z).$$

Покажем, что рациональное выражение

$$p(x,y,z)=\frac{(\lambda_1^2x+\lambda_1y+z)(\lambda_3^2x+\lambda_3y+z)}{(\lambda_2^2x+\lambda_2y+z)^2}, \tag{2}$$

где $\lambda_1=\sqrt[3]{2}$, $\lambda_2=\sqrt[3]{2}\,\varepsilon$, $\lambda_3=\sqrt[3]{2}\varepsilon^2$, а $\varepsilon=\cos\left(\frac{2\pi}{3}\right)+i\sin\left(\frac{2\pi}{3}\right)$ — первообразный корень степени 3 из 1 — L-инвариант этого оператора:

$$p(A(x,y,z)^T)=\frac{(\lambda_1^2y+\lambda_1z+2x)(\lambda_3^2y+\lambda_3z+2x)}{(\lambda_2^2y+\lambda_2z+2x)^2}=$$

$$=\frac{\lambda_1(\lambda_1y+z+\lambda_1^2x)\lambda_3(\lambda_3y+z+\lambda_3^2x)}{\lambda_2^2(\lambda_2y+z+\lambda_2^2x)^2}=$$

$$=\frac{\lambda_1\lambda_3}{\lambda_2^2}\frac{(\lambda_1^2x+\lambda_1y+z)(\lambda_3^2x+\lambda_3y+z)}{(\lambda_2^2x+\lambda_2y+z)^2}=\frac{(\lambda_1^2x+\lambda_1y+z)(\lambda_3^2x+\lambda_3y+z)}{(\lambda_2^2x+\lambda_2y+z)^2}.$$

Определение 2. Пусть $X=(x_1,\dots,x_n)$, $b=(b_1,\dots,b_n)$ — два набора переменных. Линейным циклом назовем фрагмент императивной программы вида

```
X := b;
While Q(X, b) do X := A*X
```

Замечание. Операторы `X:=b`, `X:=A*X` интерпретируются как одновременные присвоения переменным левых частей значений правых частей. В дальнейшем условие `Q(X, b)` будем игнорировать, считая линейный цикл бесконечным, а его выполнение недетерминированным. Таким образом, рассматриваются циклы вида

```
X := b;
While True|False do X := A*X
```

Предложение 1. Если $p(X)=\dfrac{r(X)}{q(X)}$ — L-инвариант линейного оператора A, многочлен $r(X)q(b)-q(X)r(b)$ — инвариант линейного цикла над полем $\overline{Q}$. Такие инварианты циклов будем также называть L-инвариантами (линейных циклов).

Пример 2 (линейный цикл с оператором примера 1). Линейный цикл, соответствующий оператору A, имеет вид

```
(x, y, z) := (a, b, c);
While True|False do (x, y, z) := (y, z, 2*x)
```

L-инвариант этого цикла определен формулой (2):

$$P(x,y,z,a,b,c) = (\lambda_1^2 x + \lambda_1 y + z)(\lambda_3^2 x + \lambda_3 y + z)(\lambda_2^2 a + \lambda_2 b + c)^2 -$$

$$-(\lambda_2^2 x + \lambda_2 y + z)^2 (\lambda_1^2 a + \lambda_1 b + c)(\lambda_3^2 a + \lambda_3 b + c). \qquad (3)$$

Отметим, что L-инвариант цикла $P(x,y,z,a,b,c)$ определен над полем $\overline{Q}(\lambda_1,\lambda_2,\lambda_3)$. Однако ему соответствует набор L-инвариантов с коэффициентами из поля Q, которые можно построить, приведя (3) к каноническому виду — многочлену от $\lambda_1,\lambda_2,\lambda_3$, затем — к многочлену от λ_2, используя соотношение $\lambda_1\lambda_3 = \lambda_2^2$ и соотношения Виета. Продемонстрируем технику вычисления L-инвариантов над полем Q.

Введем обозначения:

$$r(x,y,z) = (\lambda_1^2 x + \lambda_1 y + z)(\lambda_3^2 x + \lambda_3 y + z), \quad q(x,y,z) = (\lambda_2^2 x + \lambda_2 y + z)^2.$$

Многочлены r, q определены над полем $Q(\lambda_2)$. Вычислив $r(x,y,z), q(x,y,z)$ в виде многочленов от λ_2, получим

$$r(x,y,z) = r_0(x,y,z) + r_1(x,y,z)\lambda_2 + r_2(x,y,z)\lambda_2^2,$$

$$q(x,y,z) = q_0(x,y,z) + q_1(x,y,z)\lambda_2 + q_2(x,y,z)\lambda_2^2,$$

где

$$r_0(x,y,z) = z^2 - 2xy, \ r_1(x,y,z) = 2x^2 - yz, \ r_2(x,y,z) = y^2 - xz,$$

$$q_0(x,y,z) = z^2 + 4xy, \ q_1(x,y,z) = x^2 + yz, \ q_2(x,y,z) = y^2 + 2xz.$$

Дробь $\dfrac{r(x,y,z)}{q(x,y,z)}$ представима в виде многочлена от λ_2 с коэффициентами из $Q(x,y,z)$:

$$\frac{r(x,y,z)}{q(x,y,z)} = \frac{r_0(x,y,z) + r_1(x,y,z)\lambda_2 + r_2(x,y,z)\lambda_2^2}{q_0(x,y,z) + q_1(x,y,z)\lambda_2 + q_2(x,y,z)\lambda_2^2} = U + V\lambda_2 + W\lambda_2^2,$$

$$U, V, W \in Q(x,y,z); \qquad (4)$$

Выражение $U(x,y,z), V(x,y,z), W(x,y,z)$ можно вычислить методом неопределенных коэффициентов, используя равенство (4). Заметим, что $U(x,y,z), V(x,y,z), W(x,y,z)$ — L-инварианты оператора A. В самом деле,

$$p(x,y,z) - p(a,b,c) = (U(x,y,z) - U(a,b,c)) + (V(x,y,z) - V(a,b,c))\lambda_2 +$$

$$+ (W(x,y,z) - W(a,b,c))\lambda_2^2.$$

Поскольку $p(b,c,2a) + p(a,b,c) = 0$, имеем

$$(U(b,c,2a) - U(a,b,c)) + (V(b,c,2a) - V(a,b,c))\lambda_2 + (W(b,c,2a) - W(a,b,c))\lambda_2^2 = 0.$$

Ввиду линейной независимости векторов $1, \lambda_2, \lambda_2^2$ над Q

$$U(b,c,2a) - U(a,b,c) = 0, \ V(b,c,2a) - V(a,b,c) = 0, \ W(b,c,2a) - W(a,b,c) = 0,$$

т.е $U(x,y,z)$, $V(x,y,z)$, $W(x,y,z)$ — L-инварианты над Q.

Отметим, что если переменным a, b, c придать числовые значения, L-инвариант преобразуется в инвариант цикла.

Метод построения L-инвариантов заключается в вычислении и анализе собственных значений и собственных векторов линейных операторов.

Предложение 2. Пусть $\lambda_1, \dots, \lambda_m$ — собственные значения линейного оператора A и $s_1, \dots, s_m$ — соответствующие им собственные векторы сопряженного оператора A^*. Предположим, что существуют такие целые числа $k_1, \dots, k_m$, что

$$\lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m} = 1 . \tag{5}$$

Тогда

$$p(X) = (s_1, X)^{k_1} \cdot \ldots \cdot (s_m, X)^{k_m} \tag{6}$$

— L-инвариант линейного оператора A.

Доказательство. Пусть $\lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m} = 1$. Тогда

$$(s_1, AX)^{k_1} \cdot \ldots \cdot (s_m, AX)^{k_m} = (s_1 A, X)^{k_1} \ldots (s_m A, X)^{k_m} = (A^* s_1, X)^{k_1} \ldots (A^* s_m, X)^{k_m} =$$

$$= (\lambda_1 s_1, X)^{k_1} \ldots (\lambda_m s_m, X)^{k_m} = \lambda_1^{k_1} \ldots \lambda_m^{k_m} (s_1, X)^{k_1} \ldots (s_m, X)^{k_m} =$$
$$= (s_1, X)^{k_1} \ldots (s_m, X)^{k_m} .$$

Соотношение (5) назовем мультипликативным соотношением (между корнями характеристического многочлена), определяющим L-инвариант (6).

Пример 3 (продолжение примера 2). Рассмотрим метод предложения 2 применительно к примеру 2. Вычислим собственные числа оператора A:

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}, \quad h(\lambda) = |A - \lambda E| = \begin{vmatrix} -\lambda & 1 & 0 \\ 0 & -\lambda & 1 \\ 2 & 0 & -\lambda \end{vmatrix} = -\lambda^3 + 2.$$

Таким образом, характеристический многочлен имеет вид $h(x) = x^3 - 2$. Его корни — $\lambda_1 = \sqrt[3]{2}$, $\lambda_2 = \sqrt[3]{2}\varepsilon$, $\lambda_3 = \sqrt[3]{2}\varepsilon^2$, $\varepsilon = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$ (ε — первообразный корень степени 3 из 1).

Вычислим далее собственные векторы матрицы $A^* = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Решим систему однородных линейных уравнений $(A^* - \lambda E)\begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$, причем вычисления будем осуществлять в поле $Q(\lambda)$ по модулю $\lambda^3 - 2$. Получим систему линейных уравнений $\begin{cases} \lambda x - 2z = 0, \\ x - \lambda y = 0, \\ y - \lambda z = 0, \end{cases}$ ранг которой равен 2. Фундаментальное решение этой системы — вектор $s = (\lambda^2, \lambda, 1)$. Собственными векторами оператора A^* являются

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

Легко установить, что $\frac{\lambda_1 \lambda_3}{\lambda_2^2} = 1$. Поэтому оператор A имеет L-инвариант, определенный равенством (2).

Следствие 1. Если характеристический (минимальный) многочлен $h(x)$ линейного оператора A имеет свободный член, равный ± 1 (т.е. $\det(A) = \pm 1$), линейный оператор A обладает L-инвариантом.

Доказательство. Пусть c — свободный член многочлена $h(x)$. Тогда $c = \lambda_1 \lambda_2 \ldots \lambda_m = \pm 1$. Поэтому либо $(s_1, X) \cdot \ldots \cdot (s_m, X)$, либо $((s_1, X) \cdot \ldots \cdot (s_m, X))^2$ — L-инвариант оператора A. Отметим, что коэффициенты этого полинома принадлежат Q, поскольку они симметричны относительно перестановок корней $\lambda_1, \ldots, \lambda_m$.

Пример 4. Цикл поворота точки плоскости (a, b) на угол $\arctan\left(\frac{4}{3}\right)$:

```
(x,y)  :=  (a,b);
While True|False do (x, y):= (4/5*x - 3/5*y, 3/5*x + 4/5*y)
```

Вычислим собственные значения и собственные векторы оператора A^*:

$$A = \begin{pmatrix} 4/5 & -3/5 \\ 3/5 & 4/5 \end{pmatrix},\ h(\lambda) = |A - \lambda E| = \begin{vmatrix} 4/5-\lambda & -3/5 \\ 3/5 & 4/5-\lambda \end{vmatrix} = \lambda^2 - \frac{8}{5}\lambda + 1,$$

$$\lambda_1 = \frac{4}{5} - i\frac{3}{5},\ \lambda_2 = \frac{4}{5} + i\frac{3}{5},\ s_1 = (i,\ 1),\ s_2 = (-i,\ 1).$$

Поскольку $\lambda_1 \lambda_2 = 1$, L-инвариант оператора A имеет вид

$$p(x, y) = (ix + y)(-ix + y) = x^2 + y^2.$$

Ему соответствует инвариант цикла $x^2 + y^2 - a^2 - b^2$.

Пример 5. Цикл вычисления последовательности Фибоначчи, начиная с пары (a, b), имеет вид

```
(x,y)  :=  (a,b);
While  True|False  do  (x,  y):=  (x  +  y,  x)
```

Вычислим собственные значения и собственные векторы оператора A^*:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ h(\lambda) = |A - \lambda E| = \begin{vmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - \lambda - 1,$$

$$\lambda_1 = \frac{1}{2} - \frac{1}{2}\sqrt{5},\quad \lambda_2 = \frac{1}{2} + \frac{1}{2}\sqrt{5},$$

$$s_1 = (\lambda_1,\ 1) = \left(\frac{1}{2} - \frac{1}{2}\sqrt{5},\ 1\right),\ s_2 = (\lambda_2,\ 1) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{5},\ 1\right).$$

Поскольку $\lambda_1 \lambda_2 = -1$, L-инвариант оператора A имеет вид

$$p(x, y) = ((\lambda_1 x + y)(\lambda_2 x + y))^2 = (x^2 - xy - y^2)^2.$$

Инвариантное соотношение цикла: $(x^2 - xy - y^2)^2 = (a^2 - ab - b^2)^2$.

Следствие 2. Если характеристический (минимальный) многочлен $h(X)$ линейного оператора A имеет вид $x^m - a$, линейный оператор обладает L-инвариантами.

Доказательство. Корни λ_i характеристического многочлена $x^m - a$ определены формулой $\lambda_i = \sqrt[m]{a}\varepsilon^i$, где ε — первообразный корень степени m из 1. Легко видеть, что если $k_1, \ldots, k_m$ — целые числа такие, что $k_1 + \ldots + k_m = 0$, то $\lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m}$ — некоторая степень ε. В самом деле,

$$\lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m} = (\sqrt[m]{a})^{\sum k_i} \varepsilon^{k_1} \varepsilon^{2k_2} \cdot \ldots \cdot \varepsilon^{mk_m} = (\sqrt[m]{a})^0 \varepsilon^K = \varepsilon^K,$$

где $K = \sum ik_i$. Поэтому произведение $\lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m}$ в подходящей степени равно 1.

Итак, L-инварианты оператора A существуют и вычисляются аналогично тому, как это сделано в примере 3. В частности, L-инвариантами оператора A являются рациональные выражения

$$p_i(X)=\left(\frac{(s_i, X)}{(s_1, X)}\right)^{K_i}, \quad i=2,\ldots, m,$$

где s_i — собственные векторы A^*, а K_i — наименьшие натуральные числа такие, что iK_i кратно m: $K_i = \mathrm{im}\ \mathrm{div}\ (\gcd(i,m))$.

СВОЙСТВА L-ИНВАРИАНТОВ ЛИНЕЙНЫХ ОТОБРАЖЕНИЙ

Рассмотрим некоторые свойства L-инвариантов линейных отображений.

Предложение 3. Пусть $h(x)$ — многочлен от переменной x с рациональными коэффициентами и $\Lambda=(\lambda_1,\ldots,\lambda_m)$ — все его корни из алгебраического замыкания $\overline{Q}$ поля Q. Рассмотрим множество $G(h)=\{x_1^{k_1}\cdot\ldots\cdot x_m^{k_m} : \lambda_1^{k_1}\cdot\ldots\cdot\lambda_m^{k_m}=1\}$ — множество мономов из поля рациональных выражений $Q(X)$ (возможно, с отрицательными степенями), которые при подстановке λ_i вместо x_i получают значение 1. Тогда $G(h)$ — мультипликативная абелева группа с конечным числом образующих.

Доказательство. Каждому моному $M(X)=x_1^{k_1}\cdot\ldots\cdot x_m^{k_m}$ поставим в соответствие бином кольца $Q[X]$ $B(X)=x_{i1}^{k_{i1}}\cdot\ldots\cdot x_{il}^{k_{il}}-x_{j1}^{k_{jl}}\cdot\ldots\cdot x_{jl}^{k_{jl}}$ следующим образом: моном $M(X)$ представим в виде дроби $\dfrac{r(X)}{q(X)}$, в числителе которой запишем степени переменных с положительными показателями, а в знаменателе — степени переменных с отрицательными показателями, взятыми со знаком «минус»: $B(X)=r(X)-q(X)$.

Группа $G(h)$, очевидно, может быть задана и множеством определенных выше биномов: $G(h)=\{r(X)-q(X) \mid r(\Lambda)-q(\Lambda)=0\}$. Во множестве биномов $G(h)$ можно выделить конечное подмножество G_B, которое образует базис идеала кольца $Q[X]$, порожденного множеством $G(h)$: $I(G_B)=I(G(h))$. Построим базис Гребнера этого идеала, опираясь на базис G_B. Легко видеть, что S-полином пары биномов также является биномом. Кроме того, редукция бинома заключается в замене $r(X)$ на $q(X)$. Поэтому процесс построения базиса Гребнера приводит к конечному множеству биномов, которое обозначим $G_{\mathrm{Gr}}(h)$. Каждый элемент $G_{\mathrm{Gr}}(h)$, в свою очередь, определяет моном рассматриваемого вида. Обозначим множество таких мономов $M_{\mathrm{Gr}}(h)$. Осталось показать, что $M_{\mathrm{Gr}}(h)$ образует множество, порождающее группу $G(h)$.

Пусть $\dfrac{r(X)}{q(X)}\in G(h)$, $r(X)\succ q(X)$. Обозначим r_i-q_i, $r_i\succ q_i$, $i=1,\ldots,k$, биномы из $G_{\mathrm{Gr}}(h)$ — элементы базиса Гребнера. (Обозначения переменных в формулах опускаем.) Поскольку $G_{\mathrm{Gr}}(h)$ — базис Гребнера, бином $r-q$ редуцируется к нулю «исчерпыванием» с помощью элементов $G_{\mathrm{Gr}}(h)$. Это означает, что на каждом шаге редуцирования существует такой номер i базисного элемента, что $r=sr_i$. Шаг редуцирования исчерпыванием состоит в преобразовании $sr_i-q\to sq_i-q$. Этому преобразованию поставим в соответствие следующее преобразование монома — элемента $G(h)$:

$$\frac{r}{q}=\frac{r_i s}{q}=\frac{r_i}{q_i}\,\frac{q_i s}{q}.$$

Таким образом, шаг редуцирования применительно к элементам $G(h)$ состоит в выделении в мономе rq^{-1} сомножителя $r_i q_i^{-1}$. Редуцированный бином, если это необходимо, следует переупорядочить так, чтобы первый его моном был больше второго. Преобразование состоит в следующем: $r-q\to q-r$. Понятно, что после этого в мономе rq^{-1} выделяются сомножители знаменателя: $r_i^{-1}q_i=(r_i q_i^{-1})^{-1}$.

Итак, показано, что процесс редуцирования исчерпыванием соответствует процессу разложения монома rq^{-1} в произведение базисных мономов (возможно, с отрицательными показателями).

Теорема доказана.

Пример 6 (продолжение примера 3). Легко видеть, что для многочлена $h(x) = x^3 - 2$ имеют место следующие мультипликативные соотношения между его корнями:

$$\lambda_1^2 = \lambda_2 \lambda_3, \quad \lambda_1 \lambda_2 = \lambda_3^2, \quad \lambda_1 \lambda_3 = \lambda_2^2, \quad \lambda_2^3 = \lambda_3^3.$$

Этим соотношениям соответствуют биномы

$$x_1^2 - x_2 x_3, \; x_1 x_2 - x_3^2, \; x_1 x_3 - x_2^2, \; x_2^3 - x_3^3,$$

которые образуют базис Гребнера идеала $I(G_B) = I(G(h))$.

Следствие 3. Пусть $h(x)$ — многочлен от переменной x с рациональными коэффициентами и $\Lambda = (\lambda_1, \ldots, \lambda_m)$ — все его корни из алгебраического замыкания $\overline{Q}$ поля Q. Рассмотрим множество $G_Q(h) = \{x_1^{k_1} \cdot \ldots \cdot x_m^{k_m} : \lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m} \in Q\}$ — множество мономов из поля рациональных выражений $Q(X)$ (возможно, с отрицательными степенями), которые при подстановке λ_i вместо x_i получают рациональные значения. Тогда $G_Q(h)$ — мультипликативная абелева группа с конечным числом образующих.

Доказательство, по сути, повторяет доказательство предложения 3. Вместо биномов вида $r(X) - q(X)$ следует рассматривать биномы вида $r(X) - cq(X)$, $c \in Q$. Более того, вместо поля Q можно рассматривать любую мультипликативную подгруппу $R \subset Q$.

Следствие 4. Множество всех L-инвариантов оператора A образует поле рациональных выражений.

Доказательство очевидно. Поле L-инвариантов оператора A, порожденное элементами $G(h)$, имеет конечное число образующих — элементов $M_{\mathrm{Gr}}(h)$.

Проблему описания всех L-инвариантов линейного оператора можно теперь уточнить как проблему построения конечного множества образующих группы $G(h)$.

Предложение 4. Пусть $p(x)$ — неприводимый над полем Q приведенный многочлен и $\{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ — множество его корней над полем $\overline{Q}$. Если между его корнями существует нетривиальное мультипликативное соотношение $\lambda_1^{k_1} \ldots \lambda_m^{k_m} = 1$ с целыми показателями $k_1, \ldots, k_m$, то свободный член a_m многочлена $f(x)$ равен ± 1 либо $\sum_{i=1}^{m} k_i = 0$.

Доказательство. Пусть Q — поле рациональных чисел, $p(x)$ — неприводимый многочлен над полем Q степени m, $m > 1$. Пусть $\{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ — множество всех корней многочлена $p(x)$. Положим $L = Q(\lambda_1, \lambda_2, \ldots, \lambda_m)$, r — степень расширения поля L над полем Q, r — число, кратное m.

1. Группа Галуа G поля L над полем Q является транзитивной группой подстановок на множестве корней многочлена $p(x)$ [15].

2. Пусть H — подгруппа группы G, состоящая из всех элементов группы G, которые корень λ_1 переводят в себя. Обозначим s порядок подгруппы H и запишем разложение группы G на левые смежные классы по подгруппе H: $G = H + g_2 H + \ldots + g_m H$. Пусть w — элемент группы G, принадлежащий смежному классу $g_i H$. Тогда, по определению левого смежного класса, $w = g_i h$, где h — некоторый элемент подгруппы H. Отсюда следует, что $h(\lambda_1) = \lambda_1$. Поэтому $w(\lambda_1) = g_i h(\lambda_1) = g_i(h(\lambda_1)) = g_i(\lambda_1)$.

Поскольку $g_i \notin H$, то $g_i(\lambda_1) \neq \lambda_1$. Так как любая подстановка g из группы Галуа G поля L над полем Q переводит корень λ_1 неприводимого многочлена $p(x)$ в корень того же многочлена, $g_i(\lambda_1) = \lambda_i$; здесь λ_i — корень многочлена $p(x)$, отличный от λ_1, $1 < i \le m$. Тогда, по доказанному, для любого элемента $w \in g_i H$ $w(\lambda_1) = g_i(\lambda_1) = \lambda_i$.

Предположим, что элемент $u \in G$, причем $u \notin H$ и $u \notin g_i H$. Как было установлено выше, $u(\lambda_1) \neq \lambda_1$.

Покажем, что $u(\lambda_1) \neq \lambda_i$. Предположим противное: $u(\lambda_1) = \lambda_i$. Тогда $g_i^{-1}(\lambda_i) = \lambda_1$. Поэтому $g_i^{-1} u(\lambda_1) = g_i^{-1}(u(\lambda_1)) = g_i^{-1}(\lambda_i) = \lambda_1$. Отсюда получаем, что $g_i^{-1} u \in H$, а значит, $u \in g_i H$. По предположению $u \notin g_i H$. Полученное противоречие доказывает, что $u(\lambda_1) \neq \lambda_i$.

Следовательно, элементы группы G, принадлежащие различным левым смежным классам по подгруппе H, переводят корень λ_1 многочлена $p(x)$ в различные корни того же многочлена. В силу транзитивности группы Галуа число левых смежных классов группы G по подгруппе G равно числу корней многочлена $p(x)$, т.е. равно m.

Покажем, что число элементов в любом смежном классе группы G по подгруппе H равно порядку подгруппы H.

В самом деле, по определению $g_i H = \{g_i h \mid h \in H\}$. Отображение $\varphi: h \to g_i h$ биективно, поэтому $|g_i H| = |H| = s$. Таким образом, из рассуждений, приведенных выше, следует, что в группе G существует в точности s элементов, которые корень λ_1 переводят в корень λ_i для любого номера i, $1 < i \le m$.

3. Покажем, что справедливо соотношение $\prod_{g \in G} g(\lambda_1) = \prod_{i=1}^{n} \lambda_i^s = \left(\prod_{i=1}^{n} \lambda_i \right)^s$. Действительно, из п. 2 следует, что $\prod_{g \in g_i H} g(\lambda_1) = \lambda_i^s$, поэтому

$$\prod_{g \in G} g(\lambda_1) = \prod_{i=1}^{n} \left(\prod_{g \in g_i H} g(\lambda_1) \right) = \prod_{i=1}^{n} \lambda_i^s = \left(\prod_{i=1}^{n} \lambda_i \right)^s.$$

Утверждение п. 3 доказано.

4. Покажем, что если U — подгруппа всех подстановок, которые оставляют неподвижным корень λ_i, $i > 1$, то $U = g_i H g_i^{-1}$. Поскольку по условию $g_i(\lambda_1) = \lambda_i$, то $g_i^{-1}(\lambda_i) = \lambda_1$. Поэтому для любого элемента $h \in H$ имеет место соотношение

$$g_i h g_i^{-1}(\lambda_i) = g_i(h(g_i^{-1}(\lambda_i))) = g_i(h(\lambda_1)) = g_i(\lambda_1) = \lambda_i.$$

Итак, любой элемент из подгруппы $g_i H g_i^{-1}$ переводит корень λ_i в себя. Имеем включение $g_i H g_i^{-1} \subset U$. Предположим теперь, что для элемента $g \in G$ справедливо равенство $g(\lambda_i) = \lambda_i$, т.е. $g \in U$. Тогда $g_i^{-1}(g(\lambda_i)) = g_i^{-1}(\lambda_i) = \lambda_1$, или $g_i^{-1}(g(g_i(\lambda_1))) = \lambda_1$. Таким образом, $g_i^{-1} g g_i = h \in H$, а тогда $g = g_i h g_i^{-1}$. Поэтому имеет место включение $U \subset g_i H g_i^{-1}$. Следовательно, $U = g_i H g_i^{-1}$.

5. Поскольку порядки сопряженных подгрупп H и $g_i H g_i^{-1}$ равны, в силу п. 3

$$\prod_{g \in G} g(\lambda_j) = \prod_{i=1}^{n} \lambda_i^s = \left(\prod_{i=1}^{n} \lambda_i \right)^s.$$

6. Если $\prod_{i=1}^{n} \lambda_i^{k_i} = 1$, то $\prod_{g \in G} g\left(\prod_{i=1}^{n} \lambda_i^{k_i} \right) = \left(\prod_{i=1}^{n} \lambda_i \right)^{s \sum k_i} = 1$.

Так как g — автоморфизм поля L, имеем

$$\prod_{g\in G} g\left(\prod_{i=1}^{n}\lambda_i^{k_i}\right)=\prod_{g\in G}\left(\prod_{i=1}^{n} g(\lambda_i^{k_i})\right)=\prod_{i=1}^{n}\left(\prod_{g\in G} g(\lambda_i^{k_i})\right)=$$

$$=\prod_{i=1}^{n}\left(\prod_{g\in G}(g(\lambda_i))^{k_i}\right)=\prod_{i=1}^{n}\left(\prod_{g\in G} g(\lambda_i)\right)^{k_i}=$$

$$=\prod_{i=1}^{n}\left(\prod_{j=1}^{n}\lambda_j^{s}\right)^{k_i}=\prod_{i=1}^{n}\left(\prod_{j=1}^{n}\lambda_j\right)^{sk_i}=\left(\prod_{j=1}^{n}\lambda_j\right)^{s\sum k_i}=1.$$

7. По формуле Виета $\prod_{j=1}^{n}\lambda_j=(-1)^n a_n$. Поэтому справедливо соотношение $(-1)^n a_n^{s\sum k_i}=1$. Следовательно, $a_n^{s\sum k_i}=(-1)^n$ и $|a_n|=1$; поскольку $a_n\in Q$, либо $a_n=\pm1$, либо $s\sum k_i=0$. Так как s — натуральное число, $\sum k_i=0$.

Определение 3. L-инварианты оператора A, определенные мультипликативным соотношением между корнями характеристического многочлена $\lambda_1\cdot\ldots\cdot\lambda_m=\pm1$, назовем целыми. L-инварианты оператора A, определенные мультипликативным соотношением $\lambda_1^{k_1}\cdot\ldots\cdot\lambda_m^{k_m}=1, \sum k_i=0$, — рациональными.

Предложение 5. Если характеристический многочлен оператора A имеет вид $h(x^k), k>1$, оператор A обладает рациональными L-инвариантами.

Доказательство. Пусть $\mu_1,\ldots,\mu_l$ — корни многочлена $h(y)$. Тогда $h(x^k)=$ $=(x^k-\mu_1)\ldots(x^k-\mu_l)$. Каждый из сомножителей вида $x^k-\mu_i$ определяет рациональные L-инварианты, которые вычисляются аналогично тому, как это сделано в следствии 2 предложения 2.

ЗАКЛЮЧЕНИЕ

Задача изучения L-инвариантов линейных операторов в настоящей статье не завершена. Наиболее интересными и важными являются следующие проблемы.

1. В работе дано общее определение L-инварианта линейного оператора и доказано предложение 2 — достаточное условие существования L-инвариантов. Возникает вопрос: все ли L-инварианты описываются мультипликативными соотношениями (5) и формулой (6) предложения 2? Иными словами, можно ли обратить предложение 2?

2. Для операторов с неприводимыми характеристическими многочленами выделены два класса, для которых существуют L-инварианты. Первый класс образуют операторы, свободные члены характеристических многочленов которых равны ±1. L-инварианты циклов для таких операторов имеют вид $p(X)=p(b)$, $p(X)\in Q[X]$. Эти инварианты названы целыми. Второй класс образуют операторы, характеристические многочлены которых имеют вид $h(x^k), k>1$. L-инварианты циклов для таких операторов имеют вид $p(X)=p(b)$, $p(X)\in Q(X)$. Эти инварианты названы рациональными. Вопрос: исчерпываются ли данными двумя классами все линейные операторы, обладающие L-инвариантами? Другими словами, все ли рациональные L-инварианты принадлежат второму классу?

3. Если характеристический многочлен $h(x)$ оператора A приводим над Q, можно построить L-инварианты для каждого неприводимого делителя $h(x)$. Кроме того, можно строить L-инварианты, опираясь на мультипликативные соотношения между свободными членами неприводимых делителей $h(x)$. Именно, если $h_i(x), i=1,\ldots,l,$ — неприводимые приведенные делители $h(x)$ и a_i — свободные

члены $h_i(x)$, то любое соотношение вида $a_1^{k_1} a_2^{k_2} \cdot \ldots \cdot a_l^{k_l} = 1$ определяет L-инвариант. Поскольку a_i — рациональные числа, задача вычисления $k_1, \ldots, k_l$ сводится к решению системы однородных линейных уравнений от неизвестных $k_1, \ldots, k_l$ в целых числах. Вопрос: все ли L-инварианты оператора A будут построены? Иными словами, как найти систему образующих группы $G(h)$ из предложения 3?

4. В [5, 7] описан алгоритм построения базиса векторного пространства всех инвариантов ограниченной степени для произвольного цикла с рациональным отображением в теле цикла. В связи с этим актуальной является задача оценки степени L-инвариантов. Рассмотрим линейный цикл вида

```
(x, y) := (a, b);
While True|False do (x,y) := (2*x, 2^n*y)
```

где n — натуральное число. Мультипликативное соотношение: $\dfrac{\lambda_1^n}{\lambda_2} = 1$. Таким образом, L-инвариант имеет вид $\dfrac{x^n}{y} = \dfrac{a^n}{b}$. Из этого следует, что степень L-инварианта зависит, вообще говоря, не только от размерности оператора A, но и от его коэффициентов.

СПИСОК ЛИТЕРАТУРЫ

1. Floyd R.W. Assigning meanings to programs // Proc. of Symp. on Applied Mathematics / J.T. Schwartz (Ed.); Amer. Math. Soc. — Providence: R.I., 1967. — **19**. — P. 19–32.
2. Hoare C.A.R. An axiomatic basis for computer programming // Comm. ACM. — 1969. — N 12(10). — P. 576–580.
3. Letichevsky A.A. About one approach to program analysis // Cybernetics. — 1979. — N 6. — P. 1–8.
4. Godlevsky A.B., Kapitonova Y.V., Krivoy S.L., Letichevsky A.A. Iterative methods of program analysis // Ibid. — 1989. — N 2. — P. 9–19.
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. Müller-Olm M., Seidl H. Precise interprocedural analysis through linear algebra // Proc. of Symp. on Principles of Programming Languages (Venice, Italy, Jan. 14–16, 2004). — New York: ACM, 2004. — P. 330–341.
7. Lvov M. About one algorithm of program polynomial invariants generation // Proc. Workshop on Invariant Generation: (Techn. rep.) / Univ. of Linz; Eds. M. Giese, T. Jebelean. — N 07–07 (RISC Report Series). — Linz (Austria), 2007. — P. 85–99 (electronic).
8. Müller-Olm M., Seidl H. Computing polynomial program invariants // Inform. Process. Lett. — 2004. — **91**, N 5. — P. 233–244.
9. Sankaranarayanan S., Sipma H., Manna Z. Non-linear loop invariant generation using Gröbner bases // Proc. of Symp. on Principles of Programming Languages (Venice, Italy, Jan. 14–16, 2004). — New York: ACM, 2004. — P. 318–329.
10. Caplain M. Finding invariant assertions for proving programs // Proc. of the Intern. Conf. on Reliable Software (Los Angeles, USA, Apr. 21–23, 1975). — New York: ACM, 1975. — P. 165–171.
11. Rodriguez-Carbonell E., Kapur D. Automatic generation of polynomial loop invariants: algebraic foundations // Proc. of Intern. Symp. on Symbolic and Algebraic Computation (Santander, Spain, July 4–7, 2004). — New York: ACM, 2004. — P. 266–273.
12. Rodriguez-Carbonell E., Kapur D. Automatic generation of polynomial invariants of bounded degree using abstract interpretation // Sci. Comput. Program. — 2007. — **64**, N 1. — P. 54–75.
13. 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, 25–29 Sept., 2005). — S.l.: IEEE Computer Soc., 2005. — P. 245–249.
14. Курош А.Г. Теория групп. — 3-е изд. — М.: Наука, 1967. — 648 с.
15. Постников М.М. Теория Галуа. — М.: Физматгиз, 1963. — 220 с.
16. Бухбергер Б. Базисы Гребнера. Алгоритмический метод в теории полиномиальных идеалов // Компьютерная алгебра. Символьные и алгебраические вычисления / Пер. с англ. под ред. Б. Бухбергера, Дж. Коллинза, Р. Лооса. — М.: Мир, 1986. — С. 331–383.

Поступила 21.04.2010