М.С. ЛЬВОВ

УДК 004.421.6

О СТРУКТУРЕ ПОЛИНОМИАЛЬНЫХ ИНВАРИАНТОВ ЛИНЕЙНЫХ ЦИКЛОВ

Аннотация. Рассмотрена задача генерации полиномиальных инвариантов итерационных циклов с оператором инициализации цикла и невырожденным линейным оператором в теле цикла. Множество таких инвариантов образует идеал кольца полиномов от переменных цикла. Приведен алгоритм вычисления базисных инвариантов для линейного оператора типа жордановой клетки, а также алгоритм вычисления базисных инвариантов диагонализируемого линейного оператора с неприводимым минимальным характеристическим полиномом. Доказана теорема о строении базиса идеала инвариантов: он состоит из базисных инвариантов жордановых клеток и базисных инвариантов диагонализируемой части рассматриваемого линейного оператора.

Ключевые слова: статический анализ программ, линейные циклы, инварианты циклов, инвариантные полиномы.

ВВЕДЕНИЕ

Задача поиска инвариантов циклов в императивных программах была поставлена в работах Р. Флойда [1] и С. Хоара [2] как ключевая проблема процесса анализа свойств программ. Существование и эффективность алгоритмов генерации программных инвариантов существенно зависят от свойств алгебр данных программы. Исследования задачи автоматической генерации программных инвариантов для различных алгебр данных выполнялись, начиная в 70-х годов прошлого века, в ИК НАН Украины. Их основные результаты изложены в [3, 4]. Наиболее важными с точки зрения практики являются числовые алгебры данных. В [5, 6] 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 методов заключается в построении алгебраических зависимостей между функциями — правыми частями оператора присваивания в теле цикла. Второй метод — метод неопределенных коэффициентов — строит все инварианты данного вида в произвольной контрольной точке программы. Шаблон инварианта задается полиномиальной формой с неопределенными коэффициентами. Метод основан на свойстве нетеровости колец полиномов многих переменных. В [7] использована та же идея 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. В [8] предложен метод вычисления полиномиальных программных инвариантов ограниченной степени в линейно-определенных (аффинных) программах, содержащих рекурсивные вызовы процедур.

Большое внимание уделяется анализу циклов в целях построения их программных инвариантов. В [9] изложен метод построения нелинейных и, вообще говоря, неполиномиальных инвариантных соотношений для линейных циклов. Метод использует обственные значения и собственные векторы линейного оператора в теле цикла. В [10] предложен метод вычисления полиномиальных инвариантов циклов в виде полиномиальных форм (template polynomlals) с использованием алгоритма вычисления базисов Гребнера.

В [11] изложены алгебраические основы задачи поиска полиномиальных инвариантов циклов. 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. В [12] авторы предложили метод генерации полиномиальных инвариантов циклов, включая вложенные циклы, а также учитывая программные условия как в виде полиномиальных равенств, так и неравенств. В [13] описан алгоритм поиска инвариантов линейных циклов в частном случае — для операторов с целыми собственными числами. Алгоритм ищет решение этой системы, зависящее от n. Алгоритм реализован в программной системе Теорема (Theorema System). В [14] предложен новый подход к задаче генерации полиномиальных инвариантов линейных циклов, основанный на понятии L-инварианта линейного оператора. Сформулирована теорема о связи L-инварианта с мультипликативным соотношением между корнями минимального многочлена линейного оператора в теле цикла, а также установлены важные свойства этого соотношения в случае, когда характеристический многочлен линейного оператора неприводим над полем рациональных чисел. В [15, 16] получено решение задачи генерации полиномиальных инвариантов линейных циклов для линейных операторов — нетривиальных жордановых клеток и в связи с этим сформулировано и изучено понятие собственного многочлена линейного оператора. Предложено обобщение теоремы о связи L-инварианта с мультипликативным соотношением между корнями минимального многочлена линейного оператора, использующее собственные многочлены линейного оператора.

В настоящей работе установлена теорема о структуре базиса идеала инвариантов линейного цикла с произвольным невырожденным линейным оператором в теле цикла, а также доказана алгоритмическая разрешимость проблемы построения этого базиса в случае, когда характеристический многочлен линейного оператора неприводим над полем рациональных чисел. Основные алгебраические определения и результаты, используемые в работе, можно найти в [17–20].

1. ПОСТАНОВКА ЗАДАЧИ

Определение 1. Пусть W — n-мерное векторное пространство на полем рациональных чисел Q и $\overline{Q}$ — алгебраическое замыкание поля Q. Пусть $X=(x_1,\dots,x_n)$ — 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

$$p(Ab)=p(b). \quad (1)$$

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

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

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

В дальнейшем условие $U(X, b)$ будем игнорировать, считая линейный цикл бесконечным, а его выполнение — недетерминированным. Таким образом, рассматриваются циклы вида

```
X := b;
While True|False do X := A * X.
```
(2)

Определение 3. Многочлен $p(X, b) \in Q[X, b]$ называется (полиномиальным) инвариантом цикла (2), если $\forall k \in Nat(p(A^k b, b) \equiv 0)$.

Замечание 2. Без ограничения общности можно считать, что $p(X, b)$ — однородный многочлен относительно совокупности переменных из $X \cup b$. Действительно, если $M_1, \ldots, M_l$, где $p = M_1 + \ldots + M_l$ — однородные многочлены разных степеней, то из $p(A^k b, b) \equiv 0$ следует $M_j(A^k, b) \equiv 0$ для любого $j = 1, 2, \ldots, l$, поскольку при упрощении $p(A^k b, b)$ взаимно уничтожаются только мономы одинаковых степеней.

Теорема 1. Если $p(X) = r(X) / q(X)$ — L-инвариант линейного оператора A, многочлен $r(X)q(b) - q(X)r(b)$ — инвариант линейного цикла (2) над полем $\overline{Q}$.

Такие инварианты циклов будем также называть L-инвариантами (линейных циклов), представленными в виде полиномов.

2. МУЛЬТИПЛИКАТИВНЫЕ СООТНОШЕНИЯ И ИНВАРИАНТЫ ДИАГОНАЛИЗИРУЕМЫХ ЛИНЕЙНЫХ ОПЕРАТОРОВ

Теорема 2. Пусть $\lambda_1, \ldots, \lambda_m$ — собственные значения линейного оператора A и $s_1, \ldots, s_m$ — соответствующие им собственные векторы сопряженного оператора A^*. Предположим, что существуют такие целые числа $k_1, \ldots, k_m$, что $\lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m} = 1$. Тогда $(s_1, X)^{k_1} \cdot \ldots \cdot (s_m, X)^{k_m}$ — L-инвариант линейного оператора A.

Доказательство см. в [1].

Множество всех полиномиальных инвариантов цикла (2) образует идеал кольца полиномов $Q[X]$.

Лемма 1. 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 и $U \subset \overline{G}$ — мультипликативная числовая группа. Рассмотрим множество $G_U(h) = \{x_1^{k_1} \ldots x_m^{k_m} : \lambda_1^{k_1} \ldots \lambda_m^{k_m} \in U\}$ — множество мономов из поля рациональных выражений $Q(X)$ (возможно, с отрицательными степенями), которые при подстановке λ_i вместо x_i получают значения из U. Тогда $G_U(h)$ — мультипликативная абелева группа с конечным числом образующих.

Доказательство леммы 1 очевидно, поскольку подгруппа абелевой группы с конечным числом образующих обладает конечным числом образующих.

Лемма 2. Пусть $I(B) \subset K[X]$ — идеал кольца полиномов над полем K, порожденный произвольным множеством биномов B. Тогда $I(B)$ обладает базисом Гребнера, состоящим из биномов.

Доказательство. Шаг пополнения, на котором основан алгоритм построения базисов Гребнера, примененный к паре биномов, в результате дает также бином.

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

Теорема 3. Пусть A — диагонализируемый линейный оператор и

$$I(b, A) = \{ p(b, X) \in Q[X] \,|\, p(b, A^k(b) \equiv 0 \ \forall k \in Nat \}$$

— идеал полиномиальных инвариантов цикла (2). Тогда $I(b, A)$ обладает базисом, состоящим из L-инвариантов, представленных в виде полиномов.

Доказательство. Рассмотрим базис $S = \{s_1, \ldots, s_m\}$ пространства W, образованный собственными векторами оператора A^*. Этот базис существует ввиду диагонализируемости оператора A. Введем новые векторы переменных X' и b' и выразим их в виде линейных комбинаций координат векторов X, b:

$$x_j = c_{j1}x'_1 + \ldots + a_{jm}x'_m, \ b_j = c_{j1}b'_1 + \ldots + c_{jm}b'_m .$$

Выполним замены переменных в полиномиальном инварианте $p(b, X) \in I(b, A)$. Получим многочлен $p(X', b')$ с коэффициентами из $Q(\lambda_1, \lambda_2, \ldots, \lambda_m)$. Представим этот многочлен в виде суммы мономов

$$p'(X', b') = C_1(b')M_1(X') + C_2(b')M_2(X') + \ldots + C_k(b')M_k(X').$$

В дальнейшем штрихи в обозначениях переменных будем опускать. Пусть Λ — вектор $(\lambda_1, \lambda_2, \ldots, \lambda_m)$. Заметим, что $M_i(AX) = M_i(\Lambda)M_i(X)$. Поэтому, если обозначить d_i число $M_i(\Lambda)$, получим

$$\begin{aligned} p(AX, b) &= d_1C_1(b)M_1(X) + d_2C_2(b)M_2(X) + \ldots + d_kC_k(b)M_k(X), \\ p(A^jX, b) &= d_1^jC_1(b)M_1(X) + d_2^jC_2(b)M_2(X) + \ldots + d_k^jC_k(b)M_k(X). \end{aligned} \tag{3}$$

Поскольку из $p(b, X) \in I(b, A)$ следует $p(b, A^jX) \in I(b, A)$ для любого натурального j, подстановка b вместо X в (3) дает

$$0 = d_1^jC_1(b)M_1(b) + d_2^jC_2(b)M_2(b) + \ldots + d_k^jC_k(b)M_k(b). \tag{4}$$

Выделим среди чисел $d_1, \ldots, d_k$ равные между собой, сгруппируем в (4) мономы с равными коэффициентами d_j, коэффициенты d_j вынесем за скобки, а полученные в скобках полиномы обозначим q_j, $j = 1, \ldots, l$:

$$d_{j1} = \ldots = d_{jk} \to d_{j1}^jC_{j1}(b)M_{j1}(b) + \ldots + d_{jk}^jC_{jk}(b)M_{jk}(b) =$$

$$= d_{j1}^j(C_{j1}(b)M_{j1}(b) + \ldots + C_{jk}(b)M_{jk}(b)),$$

$$q_j(b) = C_{j1}(b)M_{j1}(b) + \ldots + C_{jk}(b)M_{jk}(b).$$

Тогда из (4) получим

$$0 = d_1^jq_1(b) + d_2^jq_2(b) + \ldots + d_l^jq_l(b). \tag{5}$$

Систему равенств (5) можно рассматривать как систему уравнений относительно $q_j(b)$. Определитель этой системы — определитель Вандермонда с коэффициентами d_i^j. Поскольку числа d_i попарно различны, этот определитель не равен нулю. Ввиду однородности системы (5) получаем, что $q_j(b) \equiv 0$. Следовательно, $q_j(b, X) = C_{j1}(b)M_{j1}(X) + \ldots + C_k(b)M_{jk}(X)$ — инварианты. Итак, инвариант $p(b, X)$ представлен в виде суммы инвариантов $q_j(b, X)$.

Пусть $q_j(b, X)$ — такой произвольный полиномиальный инвариант. Представим его в виде суммы мономов $q(b, X) = C_1(b)M_1(X) + C_2(b)M_2(X) + \ldots$ $\ldots + C_l(b)M_l(X)$. Поскольку $q(b, b) = 0$, для любого монома $C_i(b)M_i(X)$ найдется такой моном $C_j(b)M_j(X)$, что $C_i(b)M_i(b) + C_j(b)M_j(b) = 0$ (мономы взаимно уничтожаются). В выражении $C_i(b)M_i(X)+C_j(b)M_j(X)$ вынесем за скобки общий множитель. Получим

$$C_i(b)M_i(X)+C_j(b)M_j(X)=C_0(b)M_0(X)(C_{0i}(b)M_{0i}(X)+C_{0j}(b)M_{0j}(X)).$$

Тогда $C_{0i}(b)M_{0i}(b)+C_{0j}(b)M_{0j}(b)=0$, причем множества переменных, от которых зависят мономы $C_{0i}(b), C_{0j}(b), M_{0i}(b), M_{0j}(b)$, попарно не пересекаются. Поэтому $C_{0i}(b)=M_{0j}(b)$, $M_{0i}(b)+C_{0j}(b)$ и сумма рассматриваемых мономов имеет вид $M_{0j}(b)M_{0i}(X)-M_{0i}(b)M_{0j}(X)$.

В соответствии с определением 1 и формулой (1) это выражение — L-инвариант в полиномиальном виде. Ввиду произвольности выбора монома $C_i(b)M_i(X)$ полиномы $q_j(b, X)$ представляются в виде линейной комбинации L-инвариантов с полиномиальными коэффициентами.

Теорема доказана.

3. ИНВАРИАНТЫ ЖОРДАНОВЫХ КЛЕТОК

В общем случае невырожденный линейный оператор A в подходящем базисе может быть представлен матрицей — жордановой формой [17]:

$$A=\begin{bmatrix} J_1(\lambda_1) & 0 & \dots & 0 \\ 0 & J_2(\lambda_2) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & J_k(\lambda_k) \end{bmatrix}, \tag{6}$$

где $J_i(\lambda_i)$ — жордановы клетки разных размеров. Жорданова клетка $J(\lambda)$ имеет вид

$$J(\lambda)=\begin{bmatrix} \lambda & 1 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ 0 & \dots & \lambda & 1 \\ 0 & \dots & 0 & \lambda \end{bmatrix}. \tag{7}$$

Теория L-инвариантов жордановых клеток изложена в [15]. Ниже приведен метод построения полной системы инвариантов жордановой клетки, не использующий понятие L-инварианта.

Пусть $J(\lambda)$ — жорданова клетка (7) размера n. Каждой строке $J(\lambda)$ поставим в соответствие переменную: пусть $X=(x_1,\dots,x_{n-2},x_{n-1},x_n)$. Введем обозначения

$$y=x_{n-1},\quad z=x_n. \tag{8}$$

Пусть m — натуральное число и $a=(a_1,\dots,a_{n-2},a_{n-1},a_n)$ — вектор переменных (вектор начальных значений). Введем обозначения $b=a_{n-1}$, $c=a_n$. Вычислив m-ю итерацию $X^{(0)}=a$; $X^{(m)}=AX^{(m)}$ в явном виде $X^{(m)}=A^m X$: $X^{(m)}=J(\lambda)^m a$, получим

$$X^{(m)}=\begin{bmatrix} \lambda^m & C_1(m) & \dots & C_{n-1}(m) \\ 0 & \lambda^m & \dots & C_{n-2}(m) \\ 0 & \dots & \lambda^m & C_1(m) \\ 0 & \dots & \dots & \lambda^m \end{bmatrix}\begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{bmatrix}, \tag{9}$$

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

Рассмотрим отдельно два равенства, соответствующие двум нижним строкам матричного равенства (9) в обозначениях (8) и вычислим m, z^m:

$$\begin{cases} y^{(m)} = \lambda^m b + m\lambda^{m-1} c, \\ z^{(m)} = \lambda^m c \end{cases} \Rightarrow \begin{cases} y^{(m)} = \lambda^m \left(b + \dfrac{1}{\lambda} mc \right), \\ \lambda^m = z^{(m)} / c. \end{cases}$$

Итак,

$$\begin{cases} m = \lambda \dfrac{cy^{(m)} - bz^{(m)}}{cz}, \\ \lambda^m = z^{(m)} / c. \end{cases} \qquad (10)$$

Рассмотрим теперь равенство, соответствующее j-й строке матричного равенства (9):

$$x_j^{(m)} = \lambda^m \left(a_j + \frac{C_1(m)}{\lambda} a_{j+1} + \ldots + \frac{C_{n-j}(m)}{\lambda^{n-j}} a_n \right). \qquad (11)$$

Подставляя значения λ^m, m из (10) в (11), получаем

$$x_j^{(m)} = \frac{z^{(m)}}{c} \left(a_j + \frac{C_1\left(\lambda \dfrac{cy^{(m)} - bz^{(m)}}{cz^{(m)}} \right)}{\lambda} a_{j+1} + \ldots + \frac{C_{n-j}\left(\lambda \dfrac{cy^{(m)} - bz^{(m)}}{cz^{(m)}} \right)}{\lambda^{n-j}} a_n \right). \qquad (12)$$

Правую часть равенства (12) обозначим $q_j(\lambda, y^{(m)}, z^{(m)})$. Поскольку $c_j(m)$ — полиномы степени j от m, причем $j \in 1 \ldots n$, и m выражено в (9) через $\lambda, y^{(m)}, z^{(m)}$, то $q_j(\lambda, y^{(m)}, z^{(m)})$ зависят только от этих переменных и не зависят от m. Следовательно, в (11) можно опустить номер итерации. Поэтому равенства

$$x_j = \frac{z}{c} \left(a_j + \frac{C_1\left(\lambda \dfrac{cy - bz}{cz} \right)}{\lambda} a_{j+1} + \ldots + \frac{C_{n-j}\left(\lambda \dfrac{cy - bz}{cz} \right)}{\lambda^{n-j}} a_n \right) \qquad (13)$$

имеют место при любых значениях номера итерации, т.е. являются инвариантами цикла (2) при $A = J(\lambda)$. Итак, $x_j - q_j(\lambda, y, z)$ — инварианты цикла с оператором — жордановой клеткой $J(\lambda)$.

В пространстве $W[X]$ введем однородные координаты и вычислим соответствующие им начальные значения:

$$u_j = x_j / z, \;\; u = y / z; \;\; e_j = a_j / c, \;\; e = b / c. \qquad (14)$$

Тогда в пространстве переменных $W(u_1, \ldots, u_{n-2}, u, z)$ (13) перепишется в виде

$$u_j = e_j + \frac{C_1(\lambda(u-e))}{\lambda} e_{j+1} + \ldots + \frac{C_{n-j}(\lambda(u-e))}{\lambda^{n-j}} e_n.$$

Инварианты $x_j - q_j(\lambda, y, z)$ можно переписать в простом виде:

$$u_j - q_j(\lambda, u, 1), \;\; j = 1, \ldots, n-2. \qquad (15)$$

Нетрудно заметить, что в системе координат (14) система полиномов (15) образует базис Гребнера идеала инвариантов цикла (2). В однородных координатах (13) преобразование $J(\lambda) \cdot X$, осуществляемое жордановой клеткой, описывается формулами

$$\begin{cases} u_1 \Leftarrow u_1 + \dfrac{1}{\lambda} u_2, \\ \ldots \\ u_{n-2} \Leftarrow u_{n-2} + \dfrac{1}{\lambda} u, \\ u \Leftarrow u + \dfrac{1}{\lambda}, \\ z \Leftarrow \lambda z. \end{cases} \qquad (16)$$

Пусть $P_j(u_j, u)$ — полиномы $P_j = u_j - q_j(\lambda, u, 1)$. Применим к этой системе преобразование (16). Рассмотрим сначала P_1:

$$P_1\left(u_1 + \frac{1}{\lambda} u_2, u + \frac{1}{\lambda}\right) =$$

$$= \left(u_1 + \frac{1}{\lambda} u_2\right) - \left(e_1 + \frac{C_1 \lambda \left(u + \frac{1}{\lambda} - e\right)}{\lambda} e_{j+1} + \ldots + \frac{C_{n-1} \lambda \left(u + \frac{1}{\lambda} - e\right)}{\lambda^{n-1}} e_n\right).$$

Поскольку $P_1\left(u_1 + \frac{1}{\lambda} u_2, u + \frac{1}{\lambda}\right)$ — инвариант цикла, полином $P_1\left(u_1 + \frac{1}{\lambda} u_2, u + \frac{1}{\lambda}\right) - P_1(u_1, u)$ — также инвариант. Ввиду того, что коэффициенты при степенях переменной u_2 $P_1\left(u_1 + \frac{1}{\lambda} u_2, u + \frac{1}{\lambda}\right) - P_1(u_1, u)$ и $\frac{1}{\lambda} P_2(u_2, u)$ совпадают,

$$P_1\left(u_1 + \frac{1}{\lambda} u_2, u + \frac{1}{\lambda}\right) = P_1(u_1, u) + \frac{1}{\lambda} P_2(u_2, u).$$

Рассуждая аналогично для других значений j, получаем систему тождественных соотношений:

$$P_j\left(u_j + \frac{1}{\lambda} u_2, u + \frac{1}{\lambda}\right) \equiv P_j(u_j, u) + \frac{1}{\lambda} P_{j+1}(u_{j+1}, u), \quad j = 1, \ldots, n-2. \qquad (17)$$

Полином $P_{n-1}(u, u)$ обладает свойством $P_{n-1}(u, u) = P_{n-1}\left(u + \frac{1}{\lambda}, u + \frac{1}{\lambda}\right)$, откуда немедленно следует $P_{n-1}(u, u) = \mathrm{const}$. Положим $\bar{u} = (u_1, \ldots, u_{n-2}, u)$. В обозначениях, использующих оператор $A = J_n(\lambda)$, действующий в пространстве однородных координат, система соотношений (17) имеет вид

$$\begin{cases} P_j(A\bar{u}) = P_1(u_j, u) + \frac{1}{\lambda} P_{j+1}(u_{j+1}, u), \\ P_{n-2}(A\bar{u}) = P_{n-2}(u_{n-2}, u) + \frac{1}{\lambda} C. \end{cases}$$

Поскольку $P_{n-2}\left(u_{n-2} + \frac{1}{\lambda} u, u + \frac{1}{\lambda}\right)$, $P_{n-1}(u, u)$ — инварианты, $P_{n-2}\left(e_{n-2} + \frac{1}{\lambda} e, e + \frac{1}{\lambda}\right) = 0$, $P_{n-2}(e_{n-2}, e) = 0$. Поэтому $P_{n-1} = 0$ и

$$\begin{cases} P_j(A\bar{u}) = P_1(u_j, u) + \frac{1}{\lambda} P_{j+1}(u_{j+1}, u), \quad j = 1, \ldots, n-3, \\ P_{n-2}(A\bar{u}) = P_{n-2}(u_{n-2}, u). \end{cases}$$

4. ТЕОРЕМА О СТРУКТУРЕ БАЗИСА ИДЕАЛА ИНВАРИАНТОВ

Рассмотрим векторное пространство $U = Q(\lambda)^d [|y, z|]$ однородных многочленов степени d от переменных y и z над полем $F(\lambda)$ рациональных функций от переменной λ, для краткости обозначенное U. Это пространство имеет размерность $d+1$ над полем $F(\lambda)$. Итак, один из базисов этого пространства — система мономов $(y^d, y^{d-1}z, \ldots, yz^{d-1}, z^d)$. Пусть

$$U = (y^d, y^{d-1}z, \ldots, yz^{d-1}, z^d). \qquad (18)$$

Введем следующие обозначения:

$$U_0=(z^d),\ U_1=(yz^{d-1},z^d),\dots,\ U_k=(y^k z^{d-k},\dots,z^d),\dots,\ U_d=U.$$

Пусть T_J — линейное преобразование пространства U, действующее на базисе (18) следующим образом:

$$T_J(y^d)=(\lambda y+z)^d,\ \dots,\ T_J(y^k z^{d-k})=(\lambda y+z)^k(\lambda z)^{d-k},\ \dots\ ,\ T_J(z^d)=\lambda^d z^d.$$

Пусть $S=T_J-\lambda^d E$. Очевидно, каждое из подпространств U_k, $0\le k\le d$, инвариантно относительно линейного преобразования S.

Лемма 3. Для любого k, $0\le k\le d-1$, справедливы следующие утверждения:

1) подпространство U_k является образом подпространства U_{k+1} под действием преобразования S, т.е. $\forall f\ (f\in U_{k+1}\Leftrightarrow S(f)\in U_k)$;

2) ядром преобразования S является подпространство U_0, т.е. $\forall f\ (f\in U_0\Leftrightarrow S(f)=0)$.

Доказательство. Первое утверждение леммы докажем индукцией по k. Непосредственно из определения S следует, что $S(z^d)=0$. Кроме того,

$$S(yz^{d-1})=(\lambda y+z)(\lambda z)^{d-1}-\lambda^d yz^{d-1}=\lambda^d yz^{d-1}+\lambda^{d-1}z^d-\lambda^d yz^{d-1}=\lambda^{d-1}z^d.$$

Отсюда имеем $S(U_1)=U_0$. Таким образом, при $k=0$ первое утверждение леммы выполняется. Предположим по индукции, что это утверждение справедливо при некотором k, $k\le d-2$. Рассмотрим подпространство U_{k+1}. По предположению индукции $S(U_{k+1})=U_k$. Так как $U_{k+1}\subset U_{k+2}$, то $U_k\subset S(U_{k+2})$. Кроме того,

$$S(y^{k+2}z^{d-k-2})=(\lambda y+z)^{k+2}(\lambda z)^{d-k-2}-\lambda^d y^{k+2}z^{d-k-2}=$$
$$=C_{k+2}^1\lambda^{d-1}y^{k+1}z^{d-k+1}+w,$$

где $w=C_{k+2}^2\lambda^{d-2}y^k z^{d-k}+\ldots+C_{k+2}^j\lambda^{d-j}y^{k+2-j}z^{d-k+j-2}+\ldots+\lambda^{d-k-2}z^d$. Очевидно, что $w\in U_k\subset S(U_{k+2})$. Отсюда следует, что

$$C_{k+2}^1\lambda^{d-1}y^{k+1}z^{d-k+1}=S(y^{k+2}z^{d-k-2})-w\in S(U_{k+2}),$$

поэтому $y^{k+1}z^{d-k+1}\in S(U_{k+2})$. Таким образом, $S(U_{k+2})\supseteq(U_k,y^{k+1}z^{d-k+1})=U_{k+1}$. Обратное включение $U_{k+1}\supseteq S(U_{k+2})$ очевидно. Следовательно, $S(U_{k+2})=U_{k+1}$. Предположение индукции оправдано, первое утверждение леммы доказано.

Поскольку $S(U)=U_{d-1}$, ранг S равен d, а значит, дефект S равен 1. Поскольку $S(z^d)=0$, то $\mathrm{Ker}\,(S)=(z^d)$.

Лемма доказана.

Следствие 1. Не существует собственных полиномов от двух переменных y, z.

Доказательство. $S(U_{k+1})=U_k\ne(0)$ для любого k.

Пусть линейный оператор A в подходящем базисе представлен матрицей — жордановой формой (6) и $J_j(\lambda_j)$ — жордановы клетки A размеров n_j, $j=1,\dots,k$. Множества переменных клетки $J_j(\lambda_j)$ обозначим $X_j=\{x_{j1},\dots x_{jn_j}\}$. Аналогично (8) для каждой клетки введем обозначения $y_j=x_{jn_j-1}$, $z_j=x_{jn_j}$. Пусть, далее, $p(b;X_1,\dots,X_k)$ — произвольный инвариантный многочлен оператора A. Перейдем к пространству, определенному однородными координатами (13) с вектором начальных значений b. Используем однородные координаты, определенные в (13) для каждой жордановой клетки $J_k(\lambda_k)$ оператора A:

$$u_{ij}=x_{ij}/z_i,\ u_i=y_i/z_i;\ e_{ij}=a_{ij}/c_i. \qquad (19)$$

В многочлене $p(e; U_1, \ldots, U_k)$ исключим все переменные, кроме u_i, z_i, $i = 1 \ldots k$, используя соотношения (19). В соответствующих двумерных подпространствах преобразование $\hat{A}$, индуцируемое оператором A, определено формулами

$$\begin{cases} u_i \Leftarrow u_i + \dfrac{1}{\lambda}, \\ z_i \Leftarrow \lambda z_i. \end{cases}$$

Полученный многочлен обозначим $p_{red}(\bar{e}; u_1, z_1; \ldots, u_k, z_k)$. Множество многочленов типа $p_{red}(\bar{e}; u_1, z_1; \ldots, u_k, z_k)$ образует идеал, который обозначим $I_{red}(A)$. Рассмотрим идеал, определенный преобразованием A_{red}, действующим в подпространстве, определенном переменными $(z_1; \ldots, z_k)$. Получили ограничение оператора A на его диагонализируемое подпространство:

$$A_{red} = \begin{bmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \lambda_k \end{bmatrix}.$$

Пусть Λ — вектор $(\lambda_1, \ldots, \lambda_k)$, Z — вектор $(z_1, \ldots, z_k)$, а $I_\Lambda(Z)$ — рассматриваемый идеал. Обозначим $GBase(I)$ базис Гребнера идеала I. Тогда имеет место следующая теорема.

Теорема 4. Базисы Гребнера идеалов $I_{red} = (A)$, $I_\Lambda(A)$ равны: $GBase(I_{red}(A)) = GBase(I_\Lambda(A))$.

Доказательство. Пусть $GBase(I_\Lambda(A)) = (p_1(Z), \ldots, p_l(Z))$ — базис $I_\Lambda(Z)$. Тогда нужно показать, что для любого $p_{red}(\bar{e}; u_1, z_1; \ldots, u_k, z_k) \in I_{red}(A)$ имеет место разложение

$$p_{red}(u_1, z_1; \ldots, u_k, z_k) = q_1(Y, Z) p_1(Z) + \ldots + q_l(Y, Z) p_l(Z).$$

Предположим, что

$$GBase(I_{red}(A)) - GBase(I_\Lambda(A)) = \{p_1(\bar{e}; u_1, z_1; \ldots, u_k, z_k), \ldots, p_k(\bar{e}; u_k, z_k)\}.$$

Рассмотрим младший многочлен базиса Гребнера $GBase(I_{red}(A))$. Предположим, что u_k — его старшая переменная. Тогда он имеет вид $p_k(\bar{e}; u_k, Z) = a_0 u_k^{d_{k1}} + \ldots + a_{d_{k1}-1} u_k + a_{d_{k1}}$, где a_j — многочлены от переменных $\bar{e}; Z$.

Вычислим $p_k(A_{red}(u_k, Z))$:

$$p_k(A_{red}(u_k, Z)) = a'_0 \left(u_k + \frac{1}{\lambda_k} \right)^{d_{k1}} + \ldots + a'_{d_{k1}-1} \left(u_k + \frac{1}{\lambda_k} \right) + a'_{d_{k1}}, \ a'_j = a_j(A_{red}(Z)).$$

Поскольку $p_k(A_{red}(u_k, Z)) \in I_{red}(A)$, существует такой многочлен $b(\bar{e}; Z)$, что $p_k(A_{red}(u_k, Z)) - d(\bar{e}; Z) p_k(u_k, A) \in I_{red}(A)$. Но старшие коэффициенты многочленов $p_k(A_{red}(u_k, Z))$, $p_k(u_k, A)$ — многочлены одной и той же степени от переменных $\bar{e}; Z$. Поэтому $b(\bar{e}; Z)$ — число и $p_k(A_{red}(u_k, Z)) - dp_k(u_k, A) \in\in I_{red}(A)$. Отсюда $\deg_{u_k}(p_k(A_{red}(u_k, Z)) - bp_k(u_k, A)) < \deg_{u_k} p_k(u_k, A)$. Ввиду того, что $p_k(\bar{e}; u_k, Z)$ — элемент базиса Гребнера, его степень минимальна, поэтому $\deg_{u_k}(p_k(A_{red}(u_k, Z)) - bp_k(u_k, A)) = 0$ и $p_k(A_{red}(u_k, Z)) = bp_k(u_k, A) + q_k(Z)$. Коэффициенты $a_j(\bar{e}; Z)$, $a'_j(\bar{e}; Z)$ приведены по модулю $I_\Lambda(A)$. Поэтому $q_k(Z)$ также приведен по модулю $I_\Lambda(A)$. Следовательно, $q_k(Z) \equiv 0$ и $p_k(A_{red}(u_k, Z) = = bp_k(u_k, A))$. Но по лемме 1 $p_k(u_k, A) \equiv 0$. Итак, $GBase(I_{red}(A))$ не содержит многочлена, зависящего от u_k.

Рассмотрим опять младший многочлен базиса Гребнера $GBase(I_{red}(A))$. Пусть u_{k-1} — его старшая переменная. Тогда $p_k(\bar{e}; u_{k-1}, Z) = a_0 u_{k-1}^{d_{k-11}} + \ldots$ $\ldots + a_{d_{k-11}-1} u_k + a_{d_{k-11}}$, где a_j — многочлены от переменных $\bar{e}; u_k, Z$. Точно так же, как и выше, вычислим $p_{k-1}(A_{red}(u_{k-1}, Z)) - bp_{k-1}(u_{k-1}, A) \in I_{red}(A)$. Повторив предыдущие рассуждения, придем в выводу, что эта разность, вообще говоря, зависит от u_k как от старшей переменной. Но поскольку $GBase(I_{red}(A))$ не содержит многочлена, зависящего от u_k, $p_{k-1}(A_{red}(u_{k-1}, Z)) \equiv bp_{k-1}(u_{k-1}, A)$. Из этого следует, что $p_{k-1}(u_{k-1}, A) \equiv 0$. Очевидно, что утверждение теоремы доказывается индукцией по j от k до 1 приведенными выше рассуждениями.

Теорема 5 (о структуре идеала инвариантов). Пусть A — произвольный невырожденный линейный оператор, представленный в подходящем базисе матрицей (6), $I_{J_1}(A), \ldots, I_{J_k}(A)$ — идеалы инвариантов его жордановых клеток, представленные в однородных координатах (19) базисами вида (15) и $I_\Lambda(A)$ — идеал инвариантов оператора A_{red}, $I(A)$ — идеал инвариантов оператора A (цикла (2)). Тогда

$$GBase(I_\Lambda(A)) = GBase(I_{J_1}(A)) \cup \ldots \cup GBase(I_{J_k}(A)) \cup GBase(I_\Lambda(A)).$$

5. АЛГОРИТМ ПОСТРОЕНИЯ МУЛЬТИПЛИКАТИВНЫХ СООТНОШЕНИЙ ДЛЯ ОПЕРАТОРА С НЕПРИВОДИМЫМ ХАРАКТЕРИСТИЧЕСКИМ МНОГОЧЛЕНОМ

Введем необходимые в дальнейшем обозначения. Пусть $f \in Q[x]$ — неприводимый многочлен и $(\lambda_1, \ldots, \lambda_n)$ — его корни в алгебраическом замыкании Q. Пусть, далее, $\Lambda = (\lambda_{j_1}, \ldots, \lambda_{j_r})$ — некоторое подмножество корней f и $K = (k_1, \ldots, k_r)$ где $k_j > 0$ — целые числа. Обозначим Λ^K моном $\lambda_{j_1^{k_1}} \ldots \lambda_{j_r^{k_r}}$:

$$\Lambda^K \overset{df}{=} \lambda_1^{k_1} \ldots \lambda_r^{k_r}, \quad X^K \overset{df}{=} x_1^{k_1} \ldots x_r^{k_r}. \tag{20}$$

В дальнейшем понадобятся обозначения векторов оснований и степеней мономов вида (20), в которых эти векторы произвольны. Если M — моном вида (18), то $Base(M)$ — множество оснований $(x_{j_1}, \ldots, x_{j_r})$, а $Deg(M)$ — множество степеней $(k_1, \ldots, k_r)$. Пусть также $\deg(M) \overset{df}{=} k_1 + \ldots + k_r$ (общая степень монома), $\operatorname{len}(M) = r$ (количество символов основания). Пусть, далее, $G(f) = \{\sigma_1, \ldots, \sigma_j, \ldots\}$ — группа Галуа многочлена $f(x)$, представленная группой подстановок его корней.

Теорема 6. Если группа мультипликативных соотношений корней неприводимого многочлена $f(x)$ нетривиальна ($MR(f) \neq (e)$), могут иметь место следующие ситуации.

1. Множество корней $\Lambda = (\lambda_1, \ldots, \lambda_n)$ разбито на некоторое число l равномощных классов $\Lambda_1, \ldots, \Lambda_l$; $\Lambda_j = \{\lambda_{(j-1)d+1}, \ldots \lambda_{jd}\}$; $j = 1, \ldots, l$. При этом $d = \operatorname{len}(\Lambda_j)$, $n = ld$. Мультипликативные соотношения из $MR(f)$ в этой ситуации имеют вид $\Lambda_j = \varepsilon_j$, $j = 1, \ldots, l$, где ε_j — корни из 1.

2. Множество корней $\Lambda = (\lambda_1, \ldots, \lambda_n)$ разбивается на некоторое число k равномощных классов $\Lambda_1, \ldots, \Lambda_l$, $\Lambda_i = \{\lambda_{(i-1)d+1}, \ldots \lambda_{id}\}$; $i = 1, \ldots, k$. При этом $d = \operatorname{len}(\Lambda_j)$, $n = kd$. Мультипликативные соотношения из $MR(f)$ в этой ситуации имеют вид $\Lambda_i = \varepsilon_{ij} \Lambda_j$, $i = 1, \ldots, l$, где ε_j — корни из 1.

Обе ситуации могут иметь место одновременно.

Доказательство (для ситуации 1). Рассмотрим множество $MR(f)$ всех мультипликативных соотношений корней многочлена $f(x)$, представленное биномами вида $L - \varepsilon R$, где L, R — мономы вида (18), а $\varepsilon \in U$. В соответствии с леммой 2 это множество содержит базис Гребнера

$$GBase(f, U) = \{L_1 - \varepsilon_1 R_1, \ldots, L_m - \varepsilon_m R_m\},$$

построенный в соответствии с лексикографическом порядком $x_1 \succ x_2 \succ \ldots \succ x_n$. Тогда $x_1 \in Base(L_1)$, т.е. $L_1 = x_1^{k_1} \cdot L_1'$. Пусть $\sigma_{1j} \in G(f)$ — подстановка, переводящая переменную x_j в x_1. Поскольку полином $f(x)$ неприводим, его группа Галуа транзитивна, иными словами, такая подстановка существует для произвольного j. Индекс подстановки σ_{1j} будем опускать для упрощения записи формул. Рассмотрим бином $\sigma(L_1 - \varepsilon_1 R_1)$. Очевидно,

$$\sigma(L_1 - \varepsilon_1 R_1) = \sigma(L_1) - \varepsilon_1(R_1) = \sigma(Base(L_1))^{Deg(L_1)} - \varepsilon_1 \sigma(Base(R_1))^{Deg(R_1)}.$$

Если $x_j \in Base(L_1)$, $\sigma(Base(L_1))^{Deg(L_1)} = Base(L_1)^{\sigma(Deg(L_1))}$, т.е. $\sigma(L_1) = x_1^{k_j} \cdot L_1''$. Поскольку $L_1 - \varepsilon_1 R_1$ — единственный элемент базиса Гребнера $GBase(f, U)$, зависящий от x_1, и $\sigma(L_1 - \varepsilon_1 R_1)$ принадлежит $MR(f)$, к этому биному может быть применена операция «исчерпывания» биномом $L_1 - \varepsilon_1 R_1$, т.е. $\sigma(L_1) = M_1 \cdot L_1$. Но, очевидно, моном L_1, как и все мономы, удовлетворяет соотношениям

$$\deg(L_1) = \deg(\sigma(L_1)), \ \operatorname{len}(L_1) = \deg(\sigma(L_1)),$$

отсюда следует $\sigma(L_1) = L_1$, поэтому $k_j = k_1$. Ввиду произвольности индекса j все показатели степеней переменных в мономе L_1 равны: $k_1 = k_2 = \ldots = k_l$, $l = \operatorname{len}(L_1)$. Кроме того, подстановка σ действует на множестве переменных $Base(L_1)$, только переставляя местами его элементы: $\sigma(Base(L_1)) = Base(L_1)$.

Рассмотрим теперь правую часть бинома $B_1 \overset{df}{=} L_1 - \varepsilon_1 R_1$ — моном R_1. Возможны следующие ситуации:

а) $R_1 = 1$, т.е. $B_1 = L_1 - \varepsilon_1$; в этой ситуации, как было показано, $B_1 = (x_1 \ldots x_l)^{k_1} - \varepsilon$ (при подходящей нумерации переменных из $Base(L_1)$). Но бином $x_1 \ldots x_l - \varepsilon^{1/k_1}$ также принадлежит $MR(f)$, поэтому $k_1 = 1$ и $B_1 = x_1 \ldots x_l - \varepsilon$;

б) $R_1 \neq 1$, т.е. $Base(R_1) \neq \varnothing$, $\operatorname{len}(R_1) \neq 0$, $\deg(R_1) > 0$. Как и в анализе монома L_1, рассмотрим переменную $x_j \in Base(R_1)$ и автоморфизм из группы $\sigma_{1j} \in G(f)$, переводящий x_j в x_1. Точно такие же рассуждения, как и для L_1, показывают, что $\sigma(R_1) = L_1$, $\sigma(L_1) = R_1'$. Отсюда следует, что

$$\operatorname{len}(R_1) = \operatorname{len}(L_1), \ \sigma(Deg(R_1)) = Deg(L_1), \ \sigma(Base(R_1)) = Base(L_1)$$

при подходящей нумерации переменных

$$R_1 = x_{l+1} \ldots x_{2l}, \ B_1 = x_1 \ldots x_l - \varepsilon x_1' \ldots x_l'.$$

Доказательство (для ситуации 2). Рассмотрим второй элемент базиса Гребнера. Пусть $B_2 = L_2 - \varepsilon R_2 \in GBase(f, U)$ и $y \in Base(L_2)$. Покажем, что $y \notin Base(L_1)$. Если предположить, что $y \in Base(L_1)$, $y = x_j$, $1 < j \leq l$, на B_2 можно подействовать подстановкой σ_{1j}:

$$\sigma(L_2 - \varepsilon R_2) = \sigma(L_2) - \varepsilon' \sigma(R_2) = x_1^{k_{21}} L_2' - \varepsilon' \sigma(R_2),$$

отсюда, поскольку $x_1^{k_{21}} L_2'$ редуцируется «исчерпыванием» биномом B_1, $\sigma(L_2) = x_1^{k_{21}} L_2' = L_1 M_2$.

Но подстановка $\sigma_{1j} \in G(f)$, как отмечалось выше, меняет местами переменные из множества $Base(L_1)$. В доказательстве для ситуации 1 показано, что $\sigma(L_1) = L_1$. Это означает, что если $\sigma(L_2) = L_1 M_2$, то $L_2 = \sigma^{-1}(L_1) \sigma^{-1}(M_2)$, т.е. $L_2 = L_1 \sigma^{-1}(M_2)$, следовательно, $x_1 \in L_2$. Это противоречит свойству базиса Гребнера. Итак, второй элемент базиса Гребнера не содержит переменных из $Base(L_1)$:

$$Base(L_1) \cap Base(L_2) = \varnothing.$$

Рассмотрим теперь множество мультипликативных соотношений $MR(f)$, не зависящих от переменных из $Base(L_1)$: $MR_2(f) = MR(f) \cap Q[x_{l+1}, \ldots, x_n]$. Это множество порождается базисом Гребнера $GBase_2(f,U) = \{L_2 - \varepsilon_2 R_2, \ldots, L_m - \varepsilon_m R_m\}$. Здесь применимы к $L_2 - \varepsilon_2 R_2$ рассуждения из доказательства для ситуации 1. Таким образом,

$$L_2 - \varepsilon_2 R_2 = x_{l+1} \ldots x_{l+l_2} - \varepsilon_2 x'_{l+1} \ldots x'_{l+l_2+1}.$$

Пусть перестановка σ переводит x_1 в x_{l+1}. Тогда $\sigma(L_1) = L_2 \cdot M_1$. Перестановка σ^{-1} переводит x_{l+1} в x_1, поэтому $\sigma^{-1}(L_2) = L_1 \cdot M_2$. Отсюда следует, что $\operatorname{len}(L_1) = \operatorname{len}(L_2)$, более того, $\sigma(B_1) = B_2, \sigma^{-1}(B_2) = B_1$.

Теорема доказана.

Замечание 3. Множество элементов базиса Гребнера $GBase(f,U)$ замкнуто относительно перестановок группы Галуа $G(f)$.

Следующие примеры показывают, что на на практике имеют место обе ситуации.

Пример 1. Пусть $p(x)$ — минимальный многочлен первообразного корня степени k из единицы и $g(x) \in Z[x]$ — неприводимый многочлен степени d с нулевым свободным членом. Рассмотрим многочлен $h(x) = p(g(x))$. Тогда множество корней многочлена $h(x)$ служит примером ситуации 1 теоремы 6. Действительно,

$$h(x) = p(g(x)) = (g(x) - \varepsilon_1)(g(x) - \varepsilon_2) \ldots (g(x) - \varepsilon_{\varphi(k)})$$

(φ — функция Эйлера, значение которой, как известно, равно количеству первообразных корней степени k из единицы). Очевидно, что для j-го сомножителя $\lambda_{j1} \cdot \lambda_{j2} \cdot \ldots \cdot \lambda_{jd} = \varepsilon_j$.

Пример 2. Пусть $g(x) = x^d + b_1 x^{d-1} + \ldots + b_{d-1} x \in Z[x]$ — многочлен степени d с нулевым свободным членом и k — натуральное число. Рассмотрим многочлен $h(x) = [g(x)]^k - a$, где a — произвольное целое число, которое нельзя представить в виде c^l, $\gcd(k, l) \neq 1$ (gcd — general common divisior). (В противном случае многочлен $[g(x)]^k - a = [g(x)]^k - c^l$ приводим.) Тогда множество корней многочлена $h(x)$ служит примером ситуации 2 теоремы 6. Итак,

$$[g(x)]^k - a = (g(x) - \sqrt[k]{a})(g(x) - \sqrt[k]{a}\,\varepsilon) \ldots (g(x) - \sqrt[k]{a}\varepsilon^{k-1}), \tag{21}$$

ε — первообразный корень степени k из 1. Пусть $\lambda_{j1}, \ldots, \lambda_{jd}$ — корни произвольного сомножителя $(g(x) - \sqrt[k]{a}\varepsilon^j)$ правой части (3). Поскольку свободный член многочлена $g(x)$ равен нулю, $\lambda_{j1} \cdot \lambda_{j2} \cdot \ldots \cdot \lambda_{jd} = \sqrt[k]{a}\varepsilon^j$. $\lambda_{j1} \cdot \lambda_{j2} \cdot \ldots \cdot \lambda_{jd} = \Lambda_j$, $x_{j1} \cdot x_{j2} \cdot \ldots \cdot x_{jd} = X_j$. Тогда $\Lambda_1 = \varepsilon^{-j} \Lambda_j$, $X_1 - \varepsilon^{-j} X_j \in Gr(h, U)$. В этом примере множество корней многочлена $h(x)$ степени $\deg(h) = kd$ разбито на k подмножеств по d элементов в каждом. Базис Гребнера соответствующего множества $MR(h)$ состоит из всех мультипликативных соотношений вида $X_j / X_1 = \varepsilon^j$.

Рассмотрим далее полином $p(x) = q([g(x)]^m)$, где $q(x) \in Q[x]$ — неприводимый многочлен с ненулевым свободным членом. Тогда $p(x)$ — также пример ситуации 2 теоремы 6. Разложим $q(x) = (x - \alpha_1) \ldots (x - \alpha_k)$ в произведение линейных сомножителей, где $\alpha_1, \ldots, \alpha_k$ — корни $q(x)$. Подстановка $g(x)$ дает $q([g(x)]^m) = ([g(x)]^m - \alpha_1) \ldots ([g(x)]^m - \alpha_k)$. Каждый из сомножителей имеет вид (21).

Теорема 7. Пусть $f(x) \in Q[x]$ — неприводимый многочлен, $\lambda_1, \ldots, \lambda_m$ — его корни и ε — корень некоторой степени n из 1:

1) если имеет место соотношение $\lambda_1 = \varepsilon$, то $f(x)$ — минимальный полином расширения $Q(\varepsilon)$ над Q;

2) если имеет место соотношение $\lambda_1 = \varepsilon\lambda_2$, то существует такой многочлен $g(x) \in Q[x]$, что $f(x) = g(x^k)$.

Доказательство. 1. Утверждение очевидно.

2. Из $\lambda_1 = \varepsilon\lambda_2$ следует $\lambda_1^n = \lambda_2^n$. Ввиду транзитивности группы Галуа многочлена $f(x)$ для любого i имеет место соотношение $\lambda_i^n = \lambda_j^n$. Таким образом, множество корней $\lambda_1, \ldots, \lambda_m$ может быть разбито на попарно непересекающиеся классы эквивалентности $\Lambda_1, \ldots, \Lambda_l$ по отношению $\lambda_i, \lambda_j \in \Lambda_d \leftrightarrow \exists k \lambda_i^k = \lambda_j^k$. Ввиду транзитивности группы Галуа многочлена $f(x)$ число k общее для всех классов эквивалентности. Обозначим α_l алгебраическое число λ_i^k для $\lambda_i \in \Lambda_d$. Построим многочлен $g(x^k) = (x^k - \alpha_1) \ldots (x^k - \alpha_l)$. Поскольку произвольный автоморфизм группы Галуа переводит множество $\alpha_1, \ldots, \alpha_l$ в себя, коэффициенты $g(x^k)$ — рациональные числа и $\deg(g(x^k) = \deg(f(x))$, поэтому $g(x^k) = f(x)$.

Теорема 8. Пусть $f(x) \in Q[x]$ — неприводимый многочлен, $\lambda_1, \ldots, \lambda_m$ — его корни. Проблема построения базиса множества образующих группы $G_U(h) = \{x_1^{k_1} \ldots x_m^{k_m} : \lambda_1^{k_1} \ldots \lambda_m^{k_m} \in U\}$, где U — группа всех корней из единицы, алгоритмически разрешима.

Доказательство. Пусть $\Sigma(k, m)$ — множество всех подмножеств мощности k множества натуральных чисел $\{1, 2, \ldots, m\}$. $|\Sigma(k, m)| = C_m^k = \dfrac{m!}{k!(m-k)!}$. Обозначим Λ_σ произведение всех корней многочлена $f(x)$ с индексами из σ: $\Lambda_\sigma = \lambda_{i_1} \cdot \ldots \cdot \lambda_{i_k}$. Рассмотрим многочлен $S(x) = \prod_{\sigma \in \Sigma(k,n)} (x - \Lambda_\sigma)$. Поскольку $S(x)$ симметрический, его коэффициенты можно вычислить известными алгоритмами [17]. По теореме 7, если имеет место ситуация 1 теоремы 6, многочлен $S(x)$ делится на минимальный полином расширения $Q(\varepsilon)$ над Q. Если же имеет место ситуация 2, многочлен $S(x)$ делится на многочлен вида $g(x^k)$.

ЗАКЛЮЧЕНИЕ

Основные результаты работы — теорема 5, в которой установлена структура базиса Гребнера идеала полиномиальных инвариантов линейного цикла с произвольным невырожденным линейным оператором в теле цикла, и теорема 8 об алгоритмической разрешимости проблемы построения базиса идеала инвариантов «диагонализируемой части» A_{red} линейного оператора A в случае неприводимости его минимального характеристического полинома. В связи с этим по теореме 5 инварианты линейного оператора можно класифицировать как внутриклеточные — присущие каждой жордановой клетке линейного оператора, и межклеточные — присущие его диагонализируемой части.

Внутриклеточные инварианты вычисляются непосредственно и быстро по формулам (12). Существование межклеточных инвариантов зависит от существования нетривиальных мультипликативных соотношений между собственными числами линейного оператора (теорема 2). Для линейных операторов с неприводимым минимальным характеристическим многочленом проблема построения базиса множества мультипликативных соотношений между его собственными числами алгоритмически разрешима, но алгоритм теоремы 8 неэффективен ввиду очень большой степени многочлена $S(x)$, который нужно раскладывать на множители.

Проблема построения базиса множества мультипликативных соотношений для произвольных линейных операторов остается открытой.

СПИСОК ЛИТЕРАТУРЫ

1. Floyd R.W. Assigning meanings to programs / J.T. Schwartz (Ed.) // Proceedings of Symposium on Applied Mathematics. — Providence: 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. Letichevskii A.A. One approach to program analysis // Cybernetics. — 1979. — **15**, N 6. — P. 775–782.
4. Godlevskii A.B., Kapitonova Yu.V., Krivoi S.L., Letichevskii A.A. Iterative methods of program analysis // Cybernetics. — 1989. — **25**, N 2. — P. 139–152.
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 no. 07-07 in RISC Report Series, University of Linz, Austria. 06 2007. Workshop Proceedings. — P. 85–99.
7. Müller-Olm M., Seidl H. Precise interprocedural analysis through linear algebra // Proc. of Symposium on Principles of Programming Languages. Venice, Italy, January 14–16, 2004. — New York: ACM, 2004. — P. 330–341.
8. Müller-Olm M., Seidl H. Computing polynomial program invariants // Inf. Process. Lett. — 2004. — **9**1, N 5. — P. 233–244.
9. Caplain M. Finding invariant assertions for proving programs // Proc. of the Intern. Conf. on Reliable Software, Los Angeles, California, April 21–23 1975. — New York: ACM, 1975. — P. 165–171.
10. 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.
11. Rodriguez-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.
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. Symposium on Symbolic and Numeric Algorithms for Scientific Computing. — Timisoara, Romania, 25–29 Sept. 2005. — IEEE Computer Society, 2005. — P. 245–249.
14. Львов М.С. Полиномиальные инварианты линейных циклов // Кибернетика и системный анализ. — 2010. — № 4. — С. 159–168.
15. Львов М.С., Крекнин В.А. Нелинейные инварианты линейных циклов и собственные полиномы линейных операторов // Там же. — 2012. — № 2. — С. 126–139.
16. Крекнин В.А., Львов М.С. Собственные полиномы линейных операторов и полиномиальные инварианты линейных циклов программ // Науковий часопис Нац. пед. ун-ту ім. М.П. Драгоманова. — Сер. 1. Фіз.-мат. науки. — 2010. — Вып. 11. — С. 150–169.
17. Ван дер Варден Б.Л. Алгебра: 2-е изд. — М.: ГРФМЛ, 1979. — 624 с.
18. Курош А.Г. Теория групп: 3-е изд. — М.: Наука, 1967. — 648 с.
19. Постников М.М. Теория Галуа. — М.: Физматгиз, 1963. — 220 с.
20. Бухбергер Б. Базисы Гребнера. Алгоритмический метод в теории полиномиальных идеалов // Компьютерная алгебра. Символьные и алгебраические вычисления / Под ред. Б. Бухбергера, Дж. Коллинза, Р. Лооса. — М.: Мир, 1986. — 392 с.

Поступила 17.03.2014