УДК 004.421.6

**М.С. ЛЬВОВ, В.А. КРЕКНИН**

# НЕЛИНЕЙНЫЕ ИНВАРИАНТЫ ЛИНЕЙНЫХ ЦИКЛОВ И СОБСТВЕННЫЕ ПОЛИНОМЫ ЛИНЕЙНЫХ ОПЕРАТОРОВ

**Ключевые слова:** *статический анализ программ, полиномиальные инварианты циклов, собственные полиномы линейных операторов, задача автоматической генерации.*

## ВВЕДЕНИЕ

Проблема 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 зависят от свойств алгебр данных, с которыми работает программа. Исследования задачи автоматической генерации программных инвариантов для различных алгебр данных выполнялись в Институте кибернетики имени В.М. Глушкова НАН Украины, начиная с 70-х годов прошлого века. Их основные результаты изложены в [3, 4]. В работе [5] описан общий алгоритм вычисления полиномиальных инвариантов в произвольной контрольной точке программы, основанный на итерационном методе [3] и методе вычисления полиномиальных инвариантов ограниченной степени.

В [6] описан алгоритм вычисления полиномиальных инвариантов ограниченной степени в программах с линейными циклами и рекурсивными вызовами процедур. В [7] предложен метод построения нелинейных и, вообще говоря, неполиномиальных инвариантных соотношений для линейных циклов. Метод использует собственные значения и собственные векторы линейного оператора в теле цикла. В [8] 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 [9] предложен алгоритм поиска инвариантов некоторых классов линейных циклов, основанный на построении системы рекуррентных соотношений от переменных цикла и параметра $n$ — числа повторений цикла. Алгоритм ищет решение этой системы, зависящее от $n$. Алгоритм реализован в программной системе Теорема (Theorema System). В [10, 11] предложен новый метод построения нового класса полиномиальных инвариантов линейных циклов, так называемых $L$-инвариантов. Настоящая работа — прямое продолжение [10, 11].

## 1. $L$-ИНВАРИАНТЫ ЛИНЕЙНЫХ ОТОБРАЖЕНИЙ И ИНВАРИАНТЫ ЛИНЕЙНЫХ ЦИКЛОВ

В [10, 11] приведено определение $L$-инварианта линейного оператора $A$ и установлена связь между $L$-инвариантами и программными инвариантами итерационных циклов, в теле которых выполняется оператор $A$. Повторим эти определения.

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

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

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

```
X := b;
While Q(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 `Q(X,b)` будем игнорировать, считая линейный цикл бесконечным, а его выполнение — недетерминированным. Таким образом, мы рассматриваем циклы вида

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

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

Такие инварианты циклов будем называть $L$-инвариантами (линейных циклов).

В [10, 11] изложены результаты, фактически связанные с собственными векторами оператора $A^T$. Сформулируем основной результат этой работы.

**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 $A^T$. Предположим, что существуют такие целые числа $k_1, \ldots, k_m$, что

$$\lambda_1^{k_1} \cdot \ldots \cdot \lambda_m^{k_m} = 1. \tag{2}$$

Тогда

$$p(X) = (s_1, X)^{k_1} \cdot \ldots \cdot (s_m, X)^{k_m} \tag{3}$$

— $L$-инвариант линейного оператора $A$.

Заметим, что в общем случае невырожденный линейный оператор $A$ в подходящем базисе может быть представлен матрицей — жордановой формой [12, 13]:

$$A = \begin{bmatrix} J_1(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_2(\lambda_2) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & J_m(\lambda_m) \end{bmatrix}, \tag{4}$$

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

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

Таким образом, теорема 2 относится только к тем строкам матрицы линейного оператора $A$, которые соответствуют собственным векторам $A$, т.е. к совокупности последних строк жордановых клеток $J_i(\lambda_i)$, $i = 1, \ldots, m$. Ниже распространим эту теорему на произвольные невырожденные линейные операторы, введя в рассмотрение жордановы клетки в целом.

## 2. СОБСТВЕННЫЕ ПОЛИНОМЫ ЖОРДАНОВЫХ КЛЕТОК

Для анализа линейных циклов линейный оператор $A$ следует рассматривать как линейное преобразование $X \leftarrow AX$ переменных $X = (x_1, \ldots, x_n)$ линейного пространства $Q^d[|X|]$ однородных полиномов некоторой степени $d$. Преобра-

зование $X \leftarrow AX$ определяет линейное преобразование пространства $Q^d[|X|]$ в себя (гомоморфизм) $T_A : Q^d[|X|] \to Q^d[|X|]$. Для $p(X) \in Q^d[|X|]$ оно задано формулой

$$T_A(p(X)) = p(AX).$$

**Определение 3.** Полином $p(X) \in Q^d[|X|]$ называется собственным полиномом линейного оператора $A$ с собственным числом $\mu \in \overline{Q}$, если $p(X)$ — собственный вектор $T_A$, т.е. $T_A(p(X)) = \mu p(X)$. Таким образом, собственный полином определяется формулой

$$p(AX) = \mu p(X). \tag{6}$$

**Замечание 2.** Понятия собственного многочлена и $L$-инварианта линейного оператора — некоторые аналоги основных понятий геометрической теории инвариантов, а именно понятий относительного и абсолютного инвариантов группы $G$ преобразований векторного пространства в том случае, когда эта группа определена как циклическая с образующим элементом $A$: $G_A = \{\dots, A^{-2}, A^{-1}, E, A, A^2, \dots\}$ [14, 15].

**Пример 1.** Пусть $\bar{s} = (s_1, \dots, s_n)$ — собственный вектор оператора $A^T$ и $\lambda$ — его собственное значение. Тогда $(\bar{s}, X) = s_1 x_1 + \dots + s_n x_n$ — собственный полином оператора $A$ с собственным числом $\lambda$.

Предположим, что линейный оператор $A$ состоит из одной жордановой клетки вида (5), которую обозначим $J_n(\lambda)$. Если размеры клетки и ее собственное значение в данном контексте не играют роли, их обозначения будем игнорировать, обозначая оператор через $J$. Приведем решение задачи построения всех собственных полиномов жордановой клетки $J_n(\lambda)$.

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

$$U = (y^d, y^{d-1}z, \dots, yz^{d-1}, z^d). \tag{7}$$

Введем следующие обозначения:

$$U_0 = (z^d), U_1 = (yz^{d-1}, z^d), \dots, U_k = (y^k z^{d-k}, \dots, z^d), \dots, U_d = U. \tag{8}$$

Пусть $T_J$ — линейное преобразование пространства $U$, действующее на базисе (7) следующим образом:

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

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

**Лемма 1.** 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 следует $S(U_1)=U_0$. 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.

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

Лемма доказана.

**Следствие.** Не существует собственных полиномов от двух переменных: $y, z$.

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

Рассмотрим однородные многочлены степени $d+1$ от переменных $(x_1, \ldots, x_d, y, z)$. Пусть $U=U_0, U_1, \ldots, U_d$ — последовательность подпространств, определенная в (8).

**Теорема 3.** Существуют система многочленов $q_j(y,z) \in U_j$, $j=1, 2, \ldots, d-1$, степени $d$ и многочлен $q_{d+1}(y,z)$ степени $d+1$ такие, что многочлен

$$p = x_1 z^d + x_2 q_1(y,z) + \ldots$$

$$\ldots + x_j q_{j-1}(y,z) + \ldots + x_d q_{d-1}(y,z) + y q_d(y,z) + q_{d+1}(y,z) \qquad (9)$$

является собственным многочленом оператора $T_J$.

**Доказательство.** Запишем выражение для многочлена $T_J(p) = p(JX)$:

$$(p(JX) = (\lambda x_1 + x_2)\lambda^d z^d + (\lambda x_2 + x_3)T(q_1(y,z)) + \ldots + (\lambda x_j + x_{j+1})T(q_{j-1}(y,z)) + \ldots$$

$$\ldots + (\lambda x^d + y)T(q_{d-1}(y,z)) + (\lambda y + z)T_d(y,z) + T(q_{d+1}(y,z)).$$

В полученном выражении раскроем скобки и перегруппируем слагаемые:

$$T(p) = [\lambda x_1 \lambda^d z^d + \lambda^d x_2 z^d] + [\lambda x_2 T(q_1(y,z)) + x_3 T(q_1(y,z))] + \ldots$$

$$\ldots + [\lambda x_j T(q_{j-1}(y,z)) + x_{j+1} T(q_{j-1}(y,z))] + \ldots + [\lambda x_d T(q_{d-1}(y,z)) +$$

$$+ y T(q_{d-1}(y,z))] + \lambda y T(q_d(y,z)) + z T(q_d(y,z)) + T(q_{d+1}(y,z)) = G + H,$$

где

$$G = \lambda^{d+1} x_1 z^d + \ldots + \lambda x_j T(q_{j-1}(y,z)) + \ldots$$

$$\ldots + \lambda x_d T(q_{d-1}(y,z)) + \lambda y T(q_d(y,z)) + T(q_{d+1}(y,z)), \qquad (10)$$

$$H = \lambda^d x_2 z^d + \ldots + x_{j+1} T(q_{j-1}(y,z)) + \ldots + y T(q_{d-1}(y,z)) + z T(q_d(y,z)). \qquad (11)$$

В правой части формулы (10) преобразуем выражение $T(q_k(y,z))$ для $k=1,2,\ldots,d$:

$$T(q_k(y,z)) = S(q_k(y,z)) + \lambda^d q_k(y,z). \qquad (12)$$

Подставим выражение $T(q_k(y,z))$ из (12) в формулу (10):

$$G = \lambda^{d+1}x_1z^d + \lambda^{d+1}x_2q_1(y,z) + \ldots + \lambda^{d+1}x_jq_{j-1}(y,z) + \ldots + \lambda^{d+1}x_dq_{d-1}(y,z) +$$

$$+ \lambda^{d+1}yq_d(y,z) + q_{d+1}(y,z) + \lambda x_2S(q_1(y,z)) + \ldots + \lambda x_jS(q_{j-1}(y,z)) + \ldots$$

$$\ldots + \lambda x_dS(q_{d-1}(y,z)) + \lambda yS(q_d(y,z)) + S(q_{d+1}(y,z)).$$

Так как

$$\lambda^{d+1}x_1z^d + \lambda^{d+1}x_2q_1(y,z) + \ldots$$

$$\ldots + \lambda^{d+1}x_dq_{d-1}(y,z) + \lambda^{d+1}yq_d(y,z) + \lambda^{d+1}q_{d+1}(y,z) = \lambda^{d+1}p,$$

то

$$G = \lambda^{d+1}p + \lambda x_2S(q_1(y,z)) + \ldots$$

$$\ldots + \lambda x_dS(q_{d-1}(y,z)) + \lambda yS(q_d(y,z)) + S(q_{d+1}(y,z)). \qquad (13)$$

Из формул (10), (11) и (13) получим

$$T(p) = \lambda^{d+1}p + \lambda x_2S(q_1(y,z)) + \ldots$$

$$\ldots + \lambda x_jS(q_{j-1}(y,z)) + \ldots + \lambda x_dS(q_{d-1}(y,z)) + \lambda yS(q_d(y,z)) +$$

$$+ S(q_{d+1}(y,z)) + \lambda^d x_2z^d + x_3T(q_1(y,z)) + \ldots$$

$$\ldots + x_{j+1}T(q_{j-1}(y,z)) + \ldots + yT(q_{d-1}(y,z)) + z \cdot T(q_d(y,z)) =$$

$$= \lambda^{d+1}p + \lambda x_2(S(q_1) + \lambda^{d-1}z^d) +$$

$$+ x_3(\lambda S(q_2) + T(q_1)) + \ldots + x_j(\lambda S(q_{j-1}) + T(q_{j-2})) + \ldots$$

$$\ldots + x_d(\lambda S(q_{d-1}) + T(q_{d-2})) + y(\lambda S(q_d) + T(q_{d-1})) + zT(q_d) + S(q_{d+1}).$$

Итак,

$$T(p) = \lambda^{d+1}p + x_2(\lambda S(q_1) + T(z^d)) +$$

$$+ x_3(\lambda S(q_2) + T(q_1)) + \ldots + x_j(\lambda S(q_{j-1}) + T(q_{j-2})) + \ldots$$

$$\ldots + x_d(\lambda S(q_{d-1}) + T(q_{d-2})) + y(\lambda S(q_d) + T(q_{d-1})) + zT(q_d) + S(q_{d+1}). \qquad (14)$$

По лемме 1 $S(U_1) = U_0$; поскольку $T(z^d) \in U_0$, то в пространстве $U_1$ существует многочлен $q_1$ такой, что $S(q_1) = -\dfrac{T(z^d)}{\lambda}$. При таком выборе многочлена $q_1$ получим, что $\lambda S(q_1) + T(z^d) = 0$. Так как $T(q_1) \in U_1$, $q_2 \in U_2$, то по лемме 1 в подпространстве $U_2$ существует такой многочлен $q_2$, что $S(q_2) = -\dfrac{T(q_1)}{\lambda}$, поэтому $\lambda S(q_2) + T(q_1) = 0$. Продолжая процесс построения многочленов $q_k$, можно точно так же доказать существование такого многочлена $q_j$, что выполняется равенство $\lambda S(q_j) + T(q_{j-1}) = 0$, $j = 3,4,\ldots,d$. Наконец, многочлен $zq_d \in U_d = (y^dz, y^{d-1}z^2, \ldots, yz^d, z^{d+1})$. По лемме 1 если $U_{d+1} = (y^{d+1}, y^dz, \ldots, yz^d, z^{d+1})$, то $S(U_{d+1}) = U_d$. Поэтому в пространстве $U_{d+1}$ существует такой многочлен $q_{d+1}(y,z)$, что $S(q_{d+1}(y,z)) = -zq_d(y,z)$. Следовательно, $zT(q_d) + S(q_{d+1}) = 0$.

Итак, если выбирать указанным способом многочлены $q_j(y,z) \in U_j$, $j = 1, 2, \ldots, d$, и $q_{d+1}(y,z)$, то в правой части формулы (14) все слагаемые, кроме первого, обратятся в 0.

Следовательно, $T(p) = \lambda^{d+1}p$, т.е. многочлен $p$ является собственным многочленом оператора $T_J$.

Теорема доказана.

**Пример 2.** Приведем последовательность собственных полиномов жордановой клетки $J_5(\lambda)$ в пространстве $W_5(v, w, x, y, z)$:

$$\mu_1 = \lambda,\ p_1 = z,$$

$$\mu_2 = \lambda^2,\ p_2 = \left(x + \frac{1}{2\lambda}\, y\right) z - \frac{1}{2}\, y^2,$$

$$\mu_3 = \lambda^3,\ p_3 = \left(w - \frac{1}{3\lambda^2}\, y\right) z^2 - (x)\, yz + \frac{1}{3}\, y^3,$$

$$\mu_4 = \lambda^4,\ p_4 = \left(v + \frac{1}{4\lambda^3}\, y\right) z^3 + \left(-w + \frac{1}{2\lambda} x + \frac{1}{8\lambda^2}\, y\right) yz^2 + \left(\frac{1}{2} x - \frac{1}{4\lambda}\, y\right) y^2 z - \frac{1}{8}\, y^4.$$

**Теорема 4.** Для жордановой клетки $J_n(\lambda)$ существует набор $B_n$, состоящий из $n-1$ собственного полинома вида (9): $B_n = < p_1, p_2, \dots, p_{n-1} >$,

$$p_1 = z,\ p_2 \in Q(\lambda)[z, y, x_{n-2}], \dots,\ p_{n-1} \in Q(\lambda)[z, y, x_1, \dots, x_{n-2}].$$

Любой собственный полином $q(X)$ жордановой клетки $J_n(\lambda)$ можно представить в виде

$$q(X) = \frac{1}{z^k} F(p_1, p_2, \dots, p_{n-1}), \tag{15}$$

где $F$ — многочлен от $n-1$ переменной с коэффициентами из $Q(\lambda)$.

**Доказательство.** Рассмотрим систему равенств

$$u_1 = p_1 = z, u_2 = p_2(z, y, x_{n-2}), \dots, u_{n-1} = p_{n-1}(z, y, x_1, \dots, x_{n-2}),$$

где $U = (u_1, \dots, u_{n-1})$ — набор переменных. Любое равенство этой системы можно преобразовать к виду

$$x_j = \frac{1}{z^{n-j-1}} f_j(y, u_j, x_{j+1}, \dots, x_{n-2}). \tag{16}$$

Пусть $q(z, y, x_1, \dots, x_{n-2})$ — произвольный собственный полином. Подставляя в $q(z, y, x_1, \dots, x_{n-2})$ последовательно значения $x_j$, $j = 1, \dots, n-1$, из (16) и приводя к общему знаменателю результаты, получаем

$$q(y, U) = \frac{1}{z^k} F(y, u_1, \dots, u_{n-1}).$$

Легко доказать по индукции, что $q(y, U)$ — взвешенно однородный полином, если собственные числа переменных $u_j$ определить как $\mu_j = \lambda^j$, а переменной $y$ — как $\lambda$. Покажем, что полином $F$ не зависит от $y$. Разложим для этого $F$ по степеням $y$. Получим $F = Q_0 y^d + \dots + Q_{k-1} y + Q_k$. Заметим, что все коэффициенты $F$ — собственные полиномы. Вычисление оператора $S = T_J - \lambda^d E$ на полиноме $F$ показывает, что $S(F)$ — полином степени $d-1$ по переменной $y$: $\deg_y(S(F)) = d-1$. Следовательно, предположение $n \neq 0$ противоречит условию теоремы. Итак, $d = 0$.

Теорема доказана.

**Замечание 3.** Отметим, что формулы (16) определяют изоморфное отображение векторного пространства однородных полиномов $Q^{(d)}[z, y, x_1, \dots, x_{n-2}]$ степени $d$ в векторное пространство собственных полиномов $Q_P(y, u_1, \dots, u_{n-1})$, элементы которого имеют вид $\frac{1}{z^k} F(y, u_1, u_2, \dots, u_{n-1})$, где $F(y, u_1, u_2, \dots, u_{n-1})$ — взвешенно-однородный полином с весами переменных

$$\text{weight}(y) = 1,\ \text{weight}(u_1) = 1, \dots, \text{weight}(u_{n-1}) = n-1.$$

Система образующих $P$ пространства $Q_P(y, u_1, \dots, u_{n-1})$ состоит из собственных полиномов и переменной $y$:

$$P = < y, p_1, p_2, \dots, p_{n-1} >.$$

В системе образующих $P$ матрица $A_P$ оператора $A$ имеет вид

$$A_P = \begin{bmatrix} \lambda^n & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda^2 & 0 & 0 \\ 0 & \cdots & 0 & \lambda & 1 \\ 0 & \cdots & 0 & 0 & \lambda \end{bmatrix}.$$

**Пример 3.** Для системы образующих примера 2 формулы обратных преобразований имеют вид:

$$x = \frac{1}{z}\left[ p_2 - \frac{1}{2\lambda} yz + \frac{1}{2} y^2 \right],$$

$$w = \frac{1}{z^2}\left[ p_3 + p_2 y + \frac{1}{3\lambda^2} yz^2 - \frac{1}{2\lambda} y^2 z + \frac{1}{6} y^3 \right],$$

$$v = \frac{1}{z^3}\left[ p_4 + p_3 y - \frac{1}{2\lambda} p_2 yz + \frac{1}{2} p_2 y^2 - \frac{1}{4\lambda^3} yz^3 + \frac{11}{24\lambda^2} y^2 z^2 - \frac{1}{4\lambda} y^3 z + \frac{1}{24} y^4 \right].$$

В качестве примера этих преобразований рассмотрим задачу выражения собственного полинома второй степени $G$ от переменных $v, w, x, y, z$ через систему образующих $z, p_2, p_3, p_4, \dots$ Пусть

$$G = vz - wy + \frac{3}{2\lambda} wz + \frac{1}{2} x^2 - \frac{1}{2\lambda} xy + \frac{1}{4\lambda^2} y^2 - \frac{1}{4\lambda^3} yz.$$

Вычислим преобразования каждого из мономов $G$. Получим:

$$vz = \frac{1}{z^2}\left[ p_4 + p_3 y - \frac{1}{2\lambda} p_2 yz + \frac{1}{2} p_2 y^2 - \frac{1}{4\lambda^3} yz^3 + \frac{11}{24\lambda^2} y^2 z^2 - \frac{1}{4\lambda} y^3 z + \frac{1}{24} y^4 \right],$$

$$-wy = \frac{1}{z^2}\left[ -p_3 y - p_2 y^2 - \frac{1}{3\lambda^2} y^2 z^2 + \frac{1}{2\lambda} y^3 z - \frac{1}{6} y^4 \right],$$

$$\frac{3}{2\lambda} wz = \frac{1}{z^2}\left[ \frac{3}{2\lambda} p_3 z + \frac{3}{2\lambda} p_2 yz + \frac{1}{2\lambda^3} yz^3 - \frac{3}{4\lambda^2} y^2 z^2 + \frac{1}{4\lambda} y^3 z \right],$$

$$\frac{1}{2} x^2 = \frac{1}{z^2}\left[ \frac{1}{2} p_2^2 - \frac{1}{2\lambda} p_2 yz + \frac{1}{2} p_2 y^2 + \frac{1}{8\lambda^2} y^2 z^2 + \frac{1}{8} y^4 - \frac{1}{4\lambda} y^3 z \right],$$

$$-\frac{1}{2\lambda} xy = z^{-2}\left[ -\frac{1}{2\lambda} p_2 yz + \frac{1}{4\lambda^2} y^2 z^2 - \frac{1}{4\lambda} y^3 z \right],$$

$$d = z^{-2}\left[ \frac{1}{4\lambda^2} y^2 z^2 - \frac{1}{4\lambda^3} yz^3 \right].$$

Просуммируем полученные равенства и выделим полином, не зависящий от $y$:

$$G = z^{-2}\left[ p_4 + \frac{3}{2\lambda} p_3 z + \frac{1}{2} p_2^2 \right].$$

Это и есть представление $G$ в системе собственных образующих $P = (z, p_2, p_3, p_4 \dots)$. Осталось проверить, что все коэффициенты при мономах, зависящих от $y$, равны 0.

### 3. МАТРИЧНАЯ ФОРМУЛИРОВКА ЗАДАЧИ И АЛГОРИТМ ВЫЧИСЛЕНИЯ СОБСТВЕННЫХ ПОЛИНОМОВ

Введем необходимые матричные обозначения. Пусть

$$J(\lambda) = J = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}, \quad \bar{J}(\lambda) = \bar{J} = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda & 1 \end{bmatrix},$$

$$U = [z^{n-1}, z^{n-2}y, \ \ldots, \ y^{n-1}z, y^{n-1}],$$

$$X = \begin{bmatrix} x_1 \\ \cdots \\ x_{n-1} \\ y \\ z \end{bmatrix}, \quad \bar{X} = \begin{bmatrix} x_1 \\ \cdots \\ x_{n-1} \\ y \end{bmatrix}, \quad Q = \begin{bmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ 0 & q_{22} & \cdots & q_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & q_{nn} \end{bmatrix},$$

$$M = \begin{bmatrix} \lambda^{n-1} & \lambda^{n-2} & \cdots & \lambda & 1 \\ 0 & C_1^1\lambda^{n-1} & \cdots & C_{n-2}^1\lambda^2 & C_{n-1}^1\lambda \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & C_{n-2}^{n-2}\lambda^{n-1} & C_{n-1}^{n-2}\lambda^{n-2} \\ 0 & 0 & \cdots & 0 & \lambda^{n-1} \end{bmatrix}, \quad m_{ij} = C_{j-1}^{i-1}\lambda^{n-i+j-1}.$$

Матрицу $M$ представим в виде $M = \lambda^{n-1}E + M_1$, где $M_1$ — верхняя треугольная матрица с нулями на главной диагонали (наддиагональная матрица). Основное определение собственного многочлена жордановой клетки имеет вид $p(JX) = \lambda^n p(X)$.

Будем искать собственный многочлен в виде $p(X) = (U, Q\bar{X})$, т.е.

$$(J(U), Q \cdot J(\bar{X})) = \lambda^n (U, Q\bar{X}).$$

В матричных обозначениях это равенство перепишется в виде $(UM, Q\bar{J}X) = \lambda^n (U, Q\bar{X})$ или

$$U(MQ\bar{J}X - \lambda^n Q\bar{X}) = 0. \tag{17}$$

Пусть $E_0 = [E, \bar{0}], E_1 = [\bar{0}, E]$:

$$E_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Тогда $\bar{J} = \lambda E_0 + E_1$, $QE_0 = [Q, \bar{0}]$, $QE_1 = [\bar{0}, Q]$, $Q\bar{J} = [\lambda Q, \bar{0}] + [\bar{0}, Q]$,

$$MQ\bar{J} = [\lambda MQ, \bar{0}] + [\bar{0}, MQ] = [(\lambda^n E + \lambda M_1)Q, \bar{0}] + [\bar{0}, MQ],$$

$$MQ\bar{J} = [\lambda^n Q, \bar{0}] + [\lambda M_1 Q, \bar{0}] + [\bar{0}, MQ], \ \Delta = [\lambda M_1 Q, \bar{0}] + [\bar{0}, MQ].$$

Матрица $M_1Q$, как и матрица $M_1$, — наддиагональная матрица. Пусть $MQ = (r_{ij})_{i,j=1}^n$. Положим $r'_{ij} = r_{ij} - \lambda^{n-1}q_{ij}$, тогда

$$[\lambda M_1 Q, \bar{0}] = \begin{bmatrix} 0 & r'_{12} & r'_{13} & \cdots & r'_{1n} & 0 \\ 0 & 0 & r'_{23} & \cdots & r'_{2n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & r'_{n-1,n} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}, \quad [\bar{0}, MQ] = \begin{bmatrix} 0 & r_{11} & r_{12} & \cdots & r_{1n} \\ 0 & 0 & r_{22} & \cdots & r_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & r_{n-1n-1} & r_{n-1,n} \\ 0 & 0 & \cdots & 0 & r_{nn} \end{bmatrix}.$$

Пусть $\Delta$ — матрица в разности $MQ\bar{J}X - \lambda^n Q\bar{X}$:

$$\Delta X = \begin{bmatrix} 0 & r'_{12}+r_{11} & r'_{13}+r_{12} & \cdots & r'_{1n}+r_{1,n-1} & r_{1n} \\ 0 & 0 & r'_{23}+r_{22} & \cdots & r'_{2n}+r_{2,n-1} & r_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & r'_{n-1,n}+r_{n-1,n-1} & r_{n-1,n} \\ 0 & 0 & 0 & \cdots & 0 & r_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_{n-1} \\ y \\ z \end{bmatrix}.$$

Обозначим для краткости через $d_{ij}$ элементы матрицы $\Delta$. Рассмотрим скалярное произведение $(U, \Delta X)$, где $U = (z^{n-1}, z^{n-2}y, \ldots, y^{n-1}z, y^{n-1})$:

$$\left(\sum_{j=2}^{n-1} d_{1j}x_j + d_{1n}y + d_{1n+1}z\right)z^{n-1} + \left(\sum_{j=3}^{n-1} d_{2j}x_j + d_{2n}y + d_{2n+1}z\right)yz^{n-2} + \ldots$$

$$\ldots + \left(\sum_{j=n-1}^{n-1} d_{nj}x_j + d_{nn}y + d_{nn+1}z\right)y^{n-1} \equiv 0.$$

Во-первых, сумма в левой части тождества не зависит от $x_1$. Во-вторых, выражения — коэффициенты при каждой из переменных $x_2, \ldots, x_{n-1}$ — тождественно равны нулю. Поскольку каждое из этих выражений — однородный полином от переменных $y, z$ с коэффициентами из множества $D = \{d_{ij} : i = 1, \ldots, n-1;\ j = 1, \ldots, n-1\}$, все коэффициенты из $D$ равны нулю. В-третьих, это означает, что

$$(d_{1n}y + d_{1n+1}z)z^{n-1} + (d_{2n}y + d_{2n+1}z)yz^{n-2} + \ldots + (d_{nn}y + d_{n,n+1}z)y^{n-1} \equiv 0,$$

$$d_{1n+1}z^n + (d_{1n} + d_{2,n+1})yz^{n-1} + (d_{2n} + d_{3,n+1})y^2z^{n-2} + \ldots + (d_{n-1,n} + d_{n,n+1})y^n \equiv 0.$$

Отсюда

$$d_{1n+1} = 0,\ d_{1n} + d_{2,n+1} = 0,\ d_{2n} + d_{3,n+1} = 0, \ldots, d_{n-1,n} + d_{n,n+1} = 0.$$

Итак, матрица $\Delta$ определяет следующие подсистемы однородных линейных уравнений относительно переменных $q_{ij}$.

**Подсистема 1:**

$d_{12} = 0, d_{13} = 0, \ldots, d_{1n-1} = 0;$
$d_{23} = 0, \ldots, d_{2n-1} = 0;$
...
$d_{n-2,n-1} = 0.$

**Подсистема 2:**

$d_{1n+1} = 0,$
$d_{1n} + d_{2,n+1} = 0,\ d_{2n} + d_{3,n+1} = 0, \ldots, d_{n-1,n} + d_{n,n+1} = 0.$

Система содержит $\frac{(n-2)(n-1)}{2} + n$ уравнений и $\frac{n(n+1)}{2}$ переменных. Для того чтобы получить систему ее фундаментальных решений, можно положить

$$(q_{11}, \ldots, q_{1n-1}) = (1,0,\ldots,0), (q_{11}, \ldots, q_{1n-1}) = (0,1\ldots,0), \ldots, (q_{11}, \ldots, q_{1n-1}) = (0,0,\ldots,1).$$

Каждое фундаментальное решение представляет соответствующий собственный полином из набора $< p_2, \ldots, p_n >$ (см. пример 2).

Система уравнений в этом случае состоит из двух подсистем, а эффективный метод заключается в том, что решается сначала подсистема 1, а затем ее решение подставляется в подсистему 2.

**Пример 4.** Вычисление собственного полинома $p_5(u, v, w, x, y, z)$:

$$J = \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & 0 & \lambda \end{bmatrix}, \; X = \begin{bmatrix} u \\ v \\ w \\ x \\ y \\ z \end{bmatrix}, \; M = \begin{bmatrix} \lambda^4 & \lambda^3 & \lambda^2 & \lambda & 1 \\ 0 & \lambda^4 & 2\lambda^3 & 3\lambda^2 & 4\lambda \\ 0 & 0 & \lambda^4 & 3\lambda^3 & 6\lambda^2 \\ 0 & 0 & 0 & \lambda^4 & 4\lambda^3 \\ 0 & 0 & 0 & 0 & \lambda^4 \end{bmatrix},$$

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & q_{15} \\ 0 & q_{22} & q_{23} & q_{24} & q_{25} \\ 0 & 0 & q_{33} & q_{34} & q_{35} \\ 0 & 0 & 0 & q_{44} & q_{45} \\ 0 & 0 & 0 & 0 & q_{55} \end{bmatrix},$$

$$MQ = \begin{bmatrix} \lambda^4 & \lambda^3 q_{22} & \lambda^3 q_{23} + \lambda^2 q_{33} & \sum\limits_{i=2}^{4} \lambda^{5-i} q_{i4} & \sum\limits_{i=1}^{5} \lambda^{5-i} q_{i5} \\ 0 & \lambda^4 q_{22} & \lambda^4 q_{23} + 2\lambda^3 q_{33} & \sum\limits_{i=1}^{3} i \lambda^{5-i} q_{i+1,4} & \sum\limits_{i=1}^{4} i \lambda^{5-i} q_{i+1,5} \\ 0 & 0 & \lambda^4 q_{33} & \lambda^4 q_{34} + 3\lambda^3 q_{44} & \lambda^4 q_{35} + 3\lambda^3 q_{45} + 6\lambda^2 q_{55} \\ 0 & 0 & 0 & \lambda^4 q_{44} & \lambda^4 q_{45} + 4\lambda^3 q_{55} \\ 0 & 0 & 0 & 0 & \lambda^4 q_{55} \end{bmatrix},$$

$$[\lambda M_1 Q, 0] = \begin{bmatrix} 0 & \lambda^4 q_{22} & \lambda^4 q_{23} + \lambda^3 q_{33} & \sum\limits_{i=2}^{4} \lambda^{6-i} q_{i4} & \sum\limits_{i=2}^{5} \lambda^{6-i} q_{i5} & 0 \\ 0 & 0 & 2\lambda^4 q_{33} & \sum\limits_{i=2}^{3} i \lambda^{6-i} q_{i+1,4} & \sum\limits_{i=2}^{4} i \lambda^{6-i} q_{i+1,5} & 0 \\ 0 & 0 & 0 & 3\lambda^4 q_{44} & 3\lambda^4 q_{45} + 6\lambda^3 q_{55} & 0 \\ 0 & 0 & 0 & 0 & 4\lambda^4 q_{55} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$[\bar{0}, MQ] = \begin{bmatrix} 0 & \lambda^4 & \lambda^3 q_{22} & \lambda^3 q_{23} + \lambda^2 q_{33} & \sum\limits_{i=2}^{4} \lambda^{5-i} q_{i4} & \sum\limits_{i=1}^{5} \lambda^{5-i} q_{i5} \\ 0 & 0 & \lambda^4 q_{22} & \lambda^4 q_{23} + 2\lambda^3 q_{33} & \sum\limits_{i=1}^{3} i \lambda^{5-i} q_{i+1,4} & \sum\limits_{i=1}^{4} i \lambda^{5-i} q_{i+1,5} \\ 0 & 0 & 0 & \lambda^4 q_{33} & \lambda^4 q_{34} + 3\lambda^3 q_{44} & \lambda^4 q_{35} + 3\lambda^3 q_{45} + 6\lambda^2 q_{55} \\ 0 & 0 & 0 & 0 & \lambda^4 q_{44} & \lambda^4 q_{45} + 4\lambda^3 q_{55} \\ 0 & 0 & 0 & 0 & 0 & \lambda^4 q_{55} \end{bmatrix}.$$

Подсистема 1 имеет вид

$$d_{12}\colon \lambda^4 q_{22} + \lambda^4 = 0,$$
$$d_{13}\colon \lambda^4 q_{23} + \lambda^3 q_{33} + \lambda^3 q_{22} = 0,$$
$$d_{14}\colon \lambda^4 q_{24} + \lambda^3 q_{34} + \lambda^2 q_{44} + \lambda^3 q_{23} + \lambda^2 q_{33} = 0,$$
$$d_{23}\colon 2\lambda^4 q_{33} + \lambda^4 q_{22} = 0,$$
$$d_{24}\colon 2\lambda^4 q_{34} + 3\lambda^3 q_{44} + \lambda^4 q_{23} + 2\lambda^3 q_{33} = 0,$$
$$d_{34}\colon 3\lambda^4 q_{44} + \lambda^4 q_{33} = 0.$$

Упрощение этой подсистемы приводит к системе

$$d_{12}\colon q_{22} + 1 = 0,$$
$$d_{13}\colon \lambda q_{23} + q_{33} + q_{22} = 0,$$
$$d_{14}\colon \lambda^2 q_{24} + \lambda q_{34} + q_{44} + \lambda q_{23} + q_{33} = 0,$$
$$d_{23}\colon 2q_{33} + q_{22} = 0,$$
$$d_{24}\colon 2\lambda q_{34} + 3q_{44} + \lambda q_{23} + 2q_{33} = 0,$$
$$d_{34}\colon 3q_{44} + q_{33} = 0.$$

Решение:

$$d_{12}\colon q_{22} = -1, \quad d_{13}\colon q_{23} = \frac{1}{2\lambda}, \quad d_{14}\colon q_{24} = -\frac{1}{3\lambda^2},$$
$$d_{23}\colon q_{33} = \frac{1}{2}, \quad d_{24}\colon q_{34} = -\frac{1}{2\lambda}, \quad d_{34}\colon q_{44} = -\frac{1}{6}.$$

Подсистема 2 имеет вид

$$\sum_{i=1}^{5} \lambda^{5-i} q_{i5} = 0,$$
$$\left(\sum_{i=2}^{5} \lambda^{6-i} q_{i5}\right) + \left(\sum_{i=2}^{4} \lambda^{5-i} q_{i4}\right) + \left(\sum_{i=1}^{4} i\lambda^{5-i} q_{i+1,5}\right) = 0,$$
$$\left(\sum_{i=2}^{4} i\lambda^{6-i} q_{i+1,5}\right) + \left(\sum_{i=1}^{3} i\lambda^{5-i} q_{i+1,4}\right) + (\lambda^4 q_{35} + 3\lambda^3 q_{45} + 6\lambda^2 q_{55}) = 0,$$
$$(3\lambda^4 q_{45} + 6\lambda^3 q_{55}) + (\lambda^4 q_{34} + 3\lambda^3 q_{44}) + (\lambda^4 q_{45} + 4\lambda^3 q_{55}) = 0,$$
$$(4\lambda^4 q_{55}) + (\lambda^4 q_{44}) + (\lambda^4 q_{55}) = 0.$$

Упрощение этой подсистемы приводит к системе

$$\lambda^4 q_{15} + \lambda^3 q_{25} + \lambda^2 q_{35} + \lambda q_{45} + q_{55} = 0,$$
$$(2\lambda^4 q_{25} + 3\lambda^3 q_{35} + 4\lambda^2 q_{45} + 5\lambda q_{55}) + (-\lambda) = 0,$$
$$(3\lambda^4 q_{35} + 6\lambda^3 q_{45} + 10\lambda^2 q_{55}) + \left(-\frac{11}{6}\lambda^2\right) = 0,$$
$$(4\lambda^4 q_{45} + 10\lambda^3 q_{55}) + (-\lambda^3) = 0, \ (5\lambda^4 q_{55}) + (-\frac{1}{6}\lambda^4) = 0.$$

Решение:

$$\lambda^4 q_{15} = -\frac{1}{5}, \ \lambda^3 q_{25} = -\frac{1}{6}, \ \lambda^2 q_{35} = \frac{1}{6}, \ \lambda q_{45} = \frac{1}{6}, \ q_{55} = \frac{1}{30}.$$

Собственный полином $P_5(u, v, w, x, y, z)$:

$$P_5 = \left(u - \frac{1}{5\lambda^4} y\right) z^4 + \left(-v + \frac{1}{2\lambda} w - \frac{1}{3\lambda^2} x - \frac{1}{6\lambda^3} y\right) y z^3 + \left(\frac{1}{2} w - \frac{1}{2\lambda} x + \frac{1}{6\lambda^2} y\right) y^2 z^2 +$$
$$+ \left(-\frac{1}{6} x + \frac{1}{6\lambda} y\right) y^3 z + \left(\frac{1}{30} y\right) y^4.$$

## 4. СОБСТВЕННЫЕ ПОЛИНОМЫ И $L$-ИНВАРИАНТЫ ЛИНЕЙНЫХ ОПЕРАТОРОВ

Пусть $A$ — произвольный невырожденный линейный оператор, действующий на векторном пространстве $Q^{(d)}[X]$ однородных многочленов как линейное преобразование переменных $f(X) \to f(AX)$, $d$ — натуральное число и $X' \subseteq X$. Множество собственных полиномов степени $d$ от переменных из $X'$ образует конечномерное векторное подпространство, которое обозначим $W(A, d, X')$. Базис этого подпространства состоит из конечного числа полиномов $(q_1, .., q_M)$.

Отметим, что для операторов — жордановых клеток — теорема 4 дает описание этого базиса через полиномы набора $(p_1, \dots, p_{n-1})$, а именно

$$q_j(X) = \frac{1}{p_1^k} F_j(p_1, p_2, \dots p_{n-1}),$$

$F_j(u_1, \dots, u_{n-1}) = a_{1j} M_{1j} + \dots + a_{K_j j} M_{K_j j}$, $a_{ij} \in Q(\lambda)$, $M_{ij}$ — мономы от переменных $(u_1, \dots, u_{n-1})$.

Пусть $M = u_1^{k_1} \dots u_{n-1}^{k_{n-1}}$ — такой моном. Тогда $d = k_{n-1}(n-1) + k_{n-2}(n-2) + \dots$ $\dots + k_1 - k$. Отметим, что базис подпространства $W(A, d, X')$ можно вычислить методом неопределенных коэффициентов, однако вычислительная сложность этого алгоритма — полином от $(d+1)^{n-1}$. Поэтому задачу эффективного конструктивного описания базиса $W(A, d, X')$ следует считать открытой.

В частности, один из вопросов можно сформулировать так: пусть множество базисных мономов задано формулой

$$B(J, d, X) = \{M \mid M = u_1^{k_1} \cdot \dots \cdot u_{n-1}^{k_{n-1}}, d = k_{n-1}(n-1) + k_{n-2}(n-2) + \dots + k_1\}.$$

Очевидно, $B(J, d, X) \subset W(J, d, X)$. Является ли это множество базисом $W(J, d, X)$? Например, является ли множество

$$p_5, zp_4, z^2 p_3, z^3 p_2, z^5, p_3 p_2, zp_2^2$$

(примеры 2, 3) базисом подпространства $W(J_5, 5, \{u, v, w, x, y, z\})$?

Для каждой жордановой клетки $J_k(\lambda_k)$ жордановой формы оператора $A$ определена своя последовательность подпространств собственных полиномов. Пусть $J$ — одна такая клетка. Тогда в обозначениях, используемых выше при рассмотрении операторов — жордановых клеток, эта последовательность имеет вид

$$W(J, 1, (z)) \subset W(J, 3, (x_{n-1}, y, z)) \subset \dots \subset W(J, n, (x_1, \dots, x_{n-1}, y, z)).$$

Собственным числом подпространства $W(J(\lambda), d, X')$ назовем число $\lambda^d$. Последовательность собственных чисел рассматриваемых подпространств имеет вид $(\lambda, \lambda^3, \dots, \lambda^n)$. Если жорданова форма оператора $A$ состоит из нескольких клеток, в определении подпространств собственных полиномов $A$, очевидно, имеет смысл рассматривать только подмножества переменных вида $X' = \bigcup_J X_i^{(J)}$, где $X_i^{(J)} \stackrel{\text{df}}{=} \{x_i^{(J)}, \dots, x_{n_J-1}^{(J)}, y^{(J)}, z^{(J)}\}$, $i \geq 1$, — подмножества переменных, соответствующих данной жордановой клетке оператора $A$, а объединение берется по всем жордановым клеткам оператора $A$.

Рассмотрим линейный оператор, образованный двумя жордановыми клетками: $J_{n_1}(\lambda_1), J_{n_2}(\lambda_2)$. Любое подпространство собственных полиномов оператора $A$ в этом случае является прямым произведением подпространств жордановых клеток:

$$W(J_{n_1}, d_1, X_1) \times W(J_{n_2}, d_2, X_2) = W(A, d_1 + d_2, X_1 \cup X_2).$$

Обозначим $\mathrm{Base}(W)$ базис подпространства $W$. Тогда

$$\mathrm{Base}(W(J_{n_1}, d_1, X_1) \times W(J_{n_2}, d_2, X_2)) =$$
$$= \mathrm{Base}(W(J_{n_1}, d_1, X_1)) \times \mathrm{Base}(W(J_{n_2}, d_2, X_2)).$$

Если

$$\mathrm{Base}(W(J_{n_1}, d_1, X_1)) = (q_{11}(X_1), \ldots, q_{1k_1}(X_1)),$$
$$\mathrm{Base}(W(J_{n_2}, d_2, X_2)) = (q_{21}(X_2), \ldots, q_{2k_2}(X_2)),$$

то

$$\mathrm{Base}(W(J_{n_1}, d_1, X_1) \times W(J_{n_2}, d_2, X_2)) = \{q_{1i}(X_1) q_{2j}(X_2),\ i = 1 \ldots k_1, j = 1 \ldots k_2\},$$

а собственное число этого подпространства равно $\lambda_1^{d_1} \lambda_2^{d_2}$. Эта конструкция непосредственно распространяется на операторы, содержащие произвольное количество жордановых клеток произвольных размеров.

Если жорданова форма линейного оператора $A$ состоит из жордановых клеток $J(\lambda_1, n_1, X_1), \ldots, J(\lambda_m, n_m, X_m)$, т.е.

$$A = J(\lambda_1, n_1, X_1) \times \ldots \times J(\lambda_m, n_m, X_m),$$

для оператора $A$ можно выделить систему подпространств собственных полиномов, каждое из которых характеризуется собственным числом $\lambda_1^{d_1} \lambda_2^{d_2} \ldots \lambda_m^{d_m}$, $d_j \le n_j$, $j = 1, \ldots, m$.

**Теорема 5.** Если собственные числа двух подпространств собственных полиномов линейного оператора $A$ равны, их сумма также образует подпространство собственных полиномов:

$$\lambda_1^{k_1} \lambda_2^{k_2} \ldots \lambda_m^{k_m} = \lambda_1^{l_1} \lambda_2^{l_2} \ldots \lambda_m^{l_m} = \mu \Rightarrow W(\mu, X_1) + W(\mu, X_2) = W(\mu, X_1 \cup X_2).$$

Доказательство очевидно.

Ниже покажем, что определение подпространств собственных полиномов — одна из наиболее важных задач теории программных инвариантов линейных операторов.

Рассмотрим теперь задачу построения $L$-инвариантов линейных операторов (см. определение 1). Пусть оператор $A$ состоит из одной жордановой клетки и $q(X)$ — собственный полином $A$ с собственным числом $\lambda^d$. Тогда рациональное выражение

$$r(X) = \frac{q(X)}{z^d}$$

— $L$-инвариант $A$. Таким образом, для жордановой клетки размера $d$ существует по крайней мере $d-2$ $L$-инварианта

$$r_3(X) = \frac{p_3(X)}{z^3}, \ldots, r_n(X) = \frac{p_d(X)}{z^d}. \qquad (18)$$

Эти инварианты будем называть внутриклеточными.

**Замечание 4.** Система $L$-инвариантов (18), определяемая через собственные многочлены, задает так называемую орбиту линейного оператора $A$ в пространстве $W$. В самом деле, если вектор $b^{(0)} = (b_1^{(0)}, \ldots, b_n^{(0)})$ выбран как начальный, последовательность векторов, заданная рекуррентным соотношением $b^{(j+1)} = Ab^{(j)}$, лежит в двумерном алгебраическом многообразии, заданном системой уравнений

$$[r_3(X) = r_3(b^{(0)})] \& \ldots \& [r_n(X) = r_n(b^{(0)})]. \qquad (19)$$

Можно ожидать, что орбита $A$, как бесконечная последовательность, лежит в одномерном многообразии, причем недостающим членом системы (19) должно быть уравнение, задаваемое $L$-инвариантом, зависящим от $y, z$. Следствие к лемме 1 показывает, что таких инвариантов не существует. Однако легко проверить,

что неалгебраическая функция

$$p_{yz} = y - \frac{1}{\lambda \ln(\lambda)} z \ln(z)$$

удовлетворяет соотношению (6): $p_{yz}(AX) = \lambda P_{yz}(X)$. Поэтому к алгебраической системе (19) можно добавить неалгебраическое уравнение, получив описание одномерного многообразия, содержащего орбиту $A$:

$$[b_n^{(0)} p_{yz}(y, z) = z p_{yz}(b_{n-1}^{(0)}, b_n^{(0)})] \& [r_3(X) = r_3(b^{(0)})] \& \ldots \& [r_n(X) = r_n(b^{(0)})].$$

Теорема 5 определяет так называемые межклеточные инварианты. Именно, пусть пространство собственных полиномов произвольного линейного оператора содержит два различных подпространства: $W_1, W_2$, с равными собственными значениями (т.е. удовлетворяют теореме 5), $q_1(X_1) \in W_1$, $q_2(X_2) \in W_2$. При этом $r(X_1 \cup X_2) = \dfrac{q_1(X_1)}{q_2(X_2)}$ — $L$-инвариант оператора $A$.

**Теорема 6.** Пусть $r(X) = \dfrac{q(X)}{s(X)}$ — $L$-инвариант линейного оператора $A$. Тогда $q(X), s(X)$ — собственные полиномы $A$ с равными собственными числами.

**Доказательство.** Будем считать, что дробь $\dfrac{q(X)}{s(X)}$ несократима:

$$r(AX) = \frac{q(AX)}{s(AX)} = r(X) = \frac{q(X)}{s(X)}.$$

Поскольку несократимые дроби в поле рациональных выражений $Q(X)$ представляются в виде отношения целых выражений единственным образом с точностью до числового множителя,

$$q(AX) = \mu q(X), s(AX) = \mu s(X).$$

Теорема доказана.

В заключение сформулируем основную теорему об $L$-инвариантах линейных операторов.

**Теорема 7.** Пусть $q_1, \ldots, q_m$ — множество всех базисных полиномов всех жордановых клеток линейного оператора $A$ и $\mu_1, \ldots, \mu_m$ — совокупность их собственных чисел. Предположим, что существуют такие целые числа $k_1, \ldots, k_m$, что

$$\mu_1^{k_1} \cdot \ldots \cdot \mu_m^{k_m} = 1. \tag{20}$$

Тогда $r(X) = q_1^{k_1} \cdot \ldots \cdot q_m^{k_m}$ — $L$-инвариант линейного оператора $A$.

Доказательство очевидно.

Таким образом, проблема описания $L$-инвариантов линейного оператора $A$ сводится к проблеме описания всех соотношений (20). В [10, 11] доказано, что это множество имеет конечный базис.

Если все собственные числа линейного оператора $A$ — рациональные числа, проблема построения этого базиса алгоритмически разрешима с помощью теоретико-числового алгоритма.

В случае, когда $\lambda_j$ — алгебраические числа, проблема построения базиса множества соотношений (2) остается открытой.

СПИСОК ЛИТЕРАТУРЫ

1. Floyd R.W. Assigning Meanings to Programs // Proceedings of Symposium on Appl. Mathemat. — 1967. — **19**. — P. 19–32.

2. Hoare C.A.R. An Axiomatic Basis for Computer Programming // Commun of the ACM. — 1969. — № 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 // Appl. Algebra in Engineer., Communic. and Comput. — 1993. — N 4. — P. 21–29.
6. 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. ACM: New York, NY, USA, 2004. — P. 330–341.
7. Caplain M. Finding invariant assertions for proving programs // Proc. of the Intern. Conf. on Reliable Software. — Los Angeles, California, April 21–23 1975. ACM: New York, NY, USA – 1975. — P. 165–171.
8. Rodriguez-Carbonell E., Kapur D. Automatic generation of polynomial loop invariants: algebraic foundations // Proc. of Intern. Symp. on Symbolic and Algebraic Comput. — Santander, Spain, July 4–7, 2004. — ACM: New York, NY, USA, 2004. — P. 266–273.
9. 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 Comput. — Timisoara, Romania, 25–29 Sept. 2005. IEEE Comput. Soc., 2005. — P. 245–249.
10. Львов М.С. Полиномиальные инварианты линейных циклов // Кибернетика и системный анализ. — 2010. — № 4. — С. 159–168.
11. Lvov M.S. Polynomial invariants for linear loops // Cybernetics and Systems Analysis. — 2010. — **46**, N 4. — P. 660–668.
12. Ван дер Варден Б.Л. Алгебра. Изд. 2-е. — М.: ГРФМЛ, 1979. — 624 с.
13. Ходж В., Пидо Д. Методы алгебраической геометрии. Т. 1. — М.: Изд-во иностр. лит., 1954. — 462 с.
14. Львов М.С. Инвариантные равенства малых степеней в программах, определенных над полем // Кибернетика, 1988. — № 1. — С. 108–110.
15. Дьедонне Ж., Керрол Дж, Мамфорд Д. Геометрическая теория инвариантов. — М.: Мир, 1974. — 280 с.

*Поступила 16.11.2010*